Universidade Estadual do Sudoeste da Bahia

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Departamento de Ciências Exatas e Tecnológicas

DISSERTAÇÃO DE MESTRADO

DOS HIERÓGLIFOS AO QR CODE: CÓDIGOS COMO FERRAMENTA NA SALA DE AULA

por

Deivison Porto de Sousa

Mestrado Profissional em Matemática - Vitória da Conquista - BA

Orientador: Prof. Dr. Júlio César dos Reis

Vitória da Conquista-BA

Outubro/2016

Deivison Porto de Sousa

Dos Hieróglifos ao QR Code: códigos como ferramenta na sala de aula

Dissertação apresentada ao Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual do Sudoeste da Bahia - UESB, como requisito parcial para a obtenção do Grau de Mestre em Matemática em Rede Nacional PROFMAT.

Orientador: Prof. Dr. Júlio César dos Reis

Vitória da Conquista-BA
Outubro/2016

S696h Sousa, Deivison Porto de.
Dos hieróglifos ao QR code: códigos como ferramenta na sala de aula / Deivison Porto de Sousa, 2016.
70f.
Orientador (a): Dr. Júlio César dos Reis.
Dissertação (mestrado) – Universidade Estadual do Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Vitória da Conquista - BA, 2016.
Referências f.69-70.
1.Criptografia aplicada a matemática. 2.Código de barra. 3.Código QR. 4. Detecção de Erros. I. Reis, Júlio César dos. II. Universidade Estadual do Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional – PROFMAT. III. T.

CDD: 512.7

Catalogação na fonte: Cristiane Cardoso Sousa – CRB 5/1843
Bibliotecária – UESB – Campus de Vitória da Conquista - BA

Deivison Porto de Sousa

Dos Hieróglifos ao QR Code: códigos como ferramenta na sala de aula

Vitória da Conquista-BA, 14/10/2016

Comissão Examinadora

Prof. Dr. Júlio César dos Reis
UESB
(Orientador)

Prof. Dr. Márcio Antônio de Andrade Bortoloti
UESB

Prof.ª Dra. Selma Rozane Vieira
IFBA

RESUMO

Dos Hieróglifos ao QR Code: códigos como ferramenta na sala de aula

Este trabalho visa apresentar a importância dos códigos em nossa vida diária, especialmente o código de barras e o código QR. Queremos associá-los a conceitos matemáticos e assim, causar maior atração e motivação nos alunos. Abordamos os aspectos históricos de alguns códigos, cifras e da criptografia. Fazendo uma abordagem ao significado de cada conceito e diferenciando-os. Ainda são apresentados alguns exemplos presentes em eventos históricos marcantes, além de algumas técnicas interessantes. Descrevemos o surgimento e desenvolvimento dos códigos de barras e códigos QR, suas estruturas e leituras, apontando para o fato de privilegiarem a rapidez na realização de tarefas e a leitura por meio de equipamentos apropriados. No caso dos QR codes, são listados alguns aplicativos que possibilitam a leitura de forma prática e sites que permitem gerá-los. Apresentamos algumas características sobre detecção e correção de erros e finalizamos com duas propostas de atividades que são a confecção de um código personalizado para alunos de uma turma específica e o reforço de conteúdos por meio da brincadeira de caça ao tesouro com códigos QR.

Palavras-chave: Código de Barras. Código QR. Detecção de Erros.

ABSTRACT

Hieroglyphics to QR Code: codes as a tool in the classroom

This work aims to present the importance of codes in our daily live, especially the bar code and the QR code. We want to associate them with mathematical concepts and thus cause greater attraction and motivation in students. We approach the historical aspects of some codes, ciphers and of the cryptography. Making an approach to the meaning of each concept and differentiating them. They are still some examples present in important historical events as well as some interesting techniques. We describe the emergence and development of the barcodes and QR codes, its structures and readings, pointing to the fact give preference to the speed in performing tasks, and the reading by means of appropriate equipment. In the case of QR codes, are listed some applications that provide reading of easy form and sites that allow to you generate them. We present some characteristics of error detection and correction and we finalized with two proposed activities that are the fabrication of a custom code for students of a particular class and the reinforcement of contents through of the game of treasure hunt with QR codes.

Keywords: Barcode. QR Code. Error Detection.

LISTA DE FIGURAS

Figura 2.1 – Segunda Carta de Beale - Única decifrada. 10
Figura 3.1 – Bulls Eye. 14
Figura 3.2 – Código UPC-A. 16
Figura 3.3 – Código Dividido por Setores. 17
Figura 3.4 – Codificação EAN-13. 20
Figura 3.5 – Estrutura do EAN-13. 21
Figura 3.6 – EAN-13 de Produtos Similares. 21
Figura 4.1 – Estrutura do QR Code. 23
Figura 4.2 – QR Code para Decodificação. 24
Figura 4.3 – Padrões de Máscara. 24
Figura 4.4 – Código Mascarado. 25
Figura 4.5 – Decodificando um QR Code. 26
Figura 4.6 – Disposição da Informação. 26
Figura 4.7 – QR Code de Texto. 30
Figura 4.8 – QR Code para Página de Internet. 31
Figura 4.9 – Datamatrix. 32
Figura 4.10–Shotcode. 32
Figura 4.11–Beetag. 33
Figura 4.12–Microsof Tag. 33
Figura 4.13–Cartão de Embarque Recebido no Celular. 34
Figura 4.14–PDF-417. 34
Figura 5.1 – Diagrama de um Sistema de Comunicação em Geral. 35
Figura 5.2 – Dígito Verificador em EAN-13. 39
Figura 5.3 – Dígito Verificador UPC-A. 40
Figura 5.4 – Código ISBN. 41
Figura 5.5 – Detecção de Erro sem Correção. 44
Figura 6.1 – Código Personalizado. 47
Figura 6.2 – Representação de Séries. 48
Figura 6.3 – Código do Aluno Pronto. 49
Figura 6.4 – Adaptações. 51
Figura 6.5 – Ajude João. 52
Figura 6.6 – Homenagem a Leibniz. 55
Figura 6.7 – Parte de Verificações. 56
Figura 6.8 – Homenagem a Gauss. 57
Figura 6.9 – Pistas do Caça ao Tesouro. 64

LISTA DE TABELAS

Tabela 5.1 – Calculando Dígito Verificador - EAN-13. 39
Tabela 5.2 – Calculando Dígito Verificador - UPC-A. 40
Tabela 5.3 – Calculando Dígito Verificador - ISBN. 42
Tabela 5.4 – Dígitos Verificação - CPF. 43
Tabela 6.1 – Caracteres Imprimíveis da Tabela ASCII. 46
Tabela 6.2 – Verificação da Sigla. 55
Tabela 6.3 – Verificação do Nome. 55
Tabela 6.4 – Verificação da Verificação. 56

LISTA DE QUADROS

Quadro 1 – Cifra de César. 6
Quadro 2 – Código Navajo. 7
Quadro 3 – Código Morse Internacional. 9
Quadro 4 – Grade Cifrante. 12
Quadro 5 – Quadrilátero DO. 12
Quadro 6 – Mensagem Cifrada. 13
Quadro 7 – Codificação das Listras. 16
Quadro 8 – Codificação de Dígitos. 17
Quadro 9 – Codificação EAN-13. 19
Quadro 10 – Distribuição de Paridade. 19
Quadro 11 – Código EAN-11 para Unidades da Federação. 42
Quadro 12 – Códigos do Tesouro. 60

SUMÁRIO

Lista de figuras . . . . . **vii**

1 – Introdução **1**

2 – Códigos, Cifras e Criptografia **4**
2.1 Os Hieróglifos 4
2.2 Códigos de Guerra 6
2.3 Um Mundo Fascinante 8
2.4 Uma Cifra Interessante 10

3 – Código de Barras **14**
3.1 A Origem do Código de Barras 14
3.2 Como Funciona o Código de Barras 15
3.3 Estrutura do Código de Barras 20

4 – QR Code **22**
4.1 A Origem do QR Code 22
4.2 Como Funciona o QR Code 22
4.3 Lendo um QR Code 23
4.4 Leitura e Geração de QR Codes 28
4.5 Outros Códigos Bidimensionais 31

5 – Um Pouco Sobre Erros **35**
5.1 Conceitos Básicos 36
5.2 Aplicações de Detectores de Erros 38
5.2.1 EAN-13 e UPC 38
5.2.2 Sistema ISBN 40
5.2.3 CPF ou EAN-11 42

6 – Sugestões de Atividades **45**
6.1 Criando Seu Código Bidimensional 45
6.1.1 Recursos 50
6.1.2 Desenvolvimentos 50
6.1.3 Modificações 51
6.1.4 Exemplificando 52
6.2 Caça ao Tesouro 58
6.2.1 Desenvolvimentos 58

6.2.2 Exemplificando 59

7 – Considerações Finais 65

Referências 67

1 INTRODUÇÃO

Sabemos que a matemática, além de uma ciência em si, permeia, possivelmente, todos os campos e áreas do conhecimento como música, medicina, comércio, comunicações, etc. Sendo essencial para quantificação, ordenação e modelagem. Mas, apesar dessa evidente e propagada presença, ainda é um desafio para muitos professores estabelecer uma aula contextualizada e atraente para um aluno que tem cada vez mais ao seu dispor ferramentas tecnológicas que além de proporcionar mais facilidade na obtenção de conhecimentos também são fontes de inúmeras distrações.

> Esse impacto da tecnologia, cujo instrumento mais relevante é hoje o computador, exigirá do ensino de Matemática um redirecionamento sob uma perspectiva curricular que favoreça o desenvolvimento de habilidades e procedimentos com os quais o indivíduo possa se reconhecer e se orientar nesse mundo do conhecimento em constante movimento. (BRASIL, 2000, p. 41).

Ainda segundo Brasil (2000), esse redirecionamento e desenvolvimento de habilidades exigirá formas de pensar e saber matemáticos que devem ser desenvolvidos ao longo do ensino, bem como a capacidade de avaliar limites, possibilidades e adequação das tecnologias em diversas situações.

Diante dessa perspectiva, escolhemos uma abordagem através do estudo dos códigos por fazerem parte de nossa vida cotidiana de muitas e variadas formas, haja vista documentos de identificação como Registro Geral (RG) e Cadastro de Pessoa Física (CPF) além de CEP, números de telefone, códigos de barras nos produtos que adquirimos e, mais recentemente, QR codes.

Para Fini (2009), a finalidade desses números e códigos é viabilizar o registro, o acompanhamento e até toda a execução de uma atividade humana, em muitos casos. A maioria desses sistemas utiliza números dada sua maior eficiência para transmissão e armazenamento de dados, além da transposição do idioma, pois são usados internacionalmente. Além disso, muitos desses códigos permitem, e até exigem, controles por meio da implementação de algoritmos nos quais a matemática envolvida é muitas vezes simples e pode ser explorada pelos professores durante o ensino básico como veremos adiante.

Para além do uso prático e imediato, é também possível relacioná-los à história e desenvolvimento da humanidade tendo em vista seu papel de destaque na preservação do conhecimento, relações entre os povos e, notadamente, conflitos. Estudando a presença de códigos durante algumas guerras percebemos uma estreita relação com a criptografia, chegando ao ponto de muitas vezes confundir-se quanto ao significado de cada uma. Nota-se que o estudo da criptografia também abre uma porta de vastas possibilidades para

abordagem em sala de aula. Porém, enquanto que os códigos são um conjuntos de sinais, um vocabulário, utilizado em comunicações, podendo ou não ser secretos, a criptografia está interessada em um conjunto de técnicas para transformar a escrita ininteligível para àqueles que originalmente não façam parte da comunicação. Neste trabalho, queremos enfatizar a presença dos códigos sem, contudo, descartar o apelo e atração gerados pela criptografia.

No capítulo 2 apresentamos uma abordagem mais ampla sobre códigos, cifras e criptografia com o objetivo de esclarecer sobre a abrangência de cada um, diferenciá-los e colocar em evidência suas relações. Enquanto os códigos modificam um conjunto de sinais para torná-los mais apropriados a um objetivo, não necessariamente secreto, a criptografia objetiva empregar técnicas para que uma mensagem se torne indecifrável para aqueles que não têm acesso às convenções combinadas. Também é objetivo desse capítulo despertar curiosidades e posturas mais receptivas ao tema, uma vez que tanto códigos, cifras e criptografia podem apresentar atributos atraentes aos alunos. Para isso, destacamos alguns fatos históricos começando pela decifração dos hieróglifos e continuando principalmente com exemplos de utilização de cifras, códigos e criptografia em guerras, tais como a Segunda Guerra Mundial, devido a importância desse marco histórico para a humanidade. Além da utilidade bélica, ainda destacamos comunicações e mistérios.

No capítulo 3 falamos da origem do código de barras e seu intuito de agilizar os cálculos das contas dos clientes na saída de uma loja. As primeiras versões não se assemelhavam com o que temos hoje e a primeira aplicação comercial só se concretizou muito tempo depois da emissão de sua patente. Ainda nesse capítulo, aprendemos sobre a leitura de códigos de barras com enfoque nos padrões mais comuns que são o UPC-A e sua ampliação, o EAN-13, devido a necessidade de internacionalização do sistema, terminando com um estudo da estrutura desse código e exemplos.

O capítulo 4 apresenta a evolução bidimensional do código de barras com enfoque no QR code (código QR). Vê-se que o objetivo não é só apresentar maior quantidade de informações de forma compacta, mas também oferecer mais opções de personalização, variedade de conteúdo e segurança com possibilidades de leitura até certo grau de dano. Por meio de um exemplo simples do código, é bastante perceptível que a leitura é muito complexa e não favorece ao "olho humano", mas sim às máquinas. Felizmente, essa dificuldade é facilmente contornada por meio da proliferação de aparelhos cada vez mais práticos e potentes. O capítulo termina com indicações de como ler e criar seus próprios QR codes de forma simples, além de alguns exemplos de outros códigos bidimensionais.

No capítulo 5 apresentamos uma rápida abordagem sobre erros. Vemos, através de uma analogia com os idiomas, que as mensagens podem sofrer interferências e terem sua compreensão comprometida e, por isso, como nem sempre se poderá adotar medidas tais como, simplesmente reenviar a mensagem, necessitamos estudar meios pelos quais se

possa checar a confiabilidade do conteúdo das mesmas e até corrigi-las, quando possível. São dados exemplos mais detalhados de códigos detectores de erros no código de barras, no CPF e no sistema ISBN por serem de fácil compreensão, práticos e de uso comum.

No capítulo 6 apresentamos duas propostas para aplicação em sala de aula. Na primeira, buscamos a confecção de um código que seja inspirado no QR code, porém tornamos sua confecção e leitura bem mais intuitiva. Embora o tamanho e as disposições dos elementos possam ser alteradas, o código é proposto de uma forma que permita uma real personalização e se torne atraente para identificação de grupos e uso por parte dos alunos, além de permitir a exploração de propriedades aritméticas, algébricas e outras dependendo da intenção e adaptação por parte do professor. A segunda atividade faz uso da conhecida brincadeira de caça ao tesouro usando códigos QR como forma de esconder as pistas. Apesar da clara adaptação dessa atividade para vários conteúdos, em ambos os casos são oferecidos exemplos práticos para facilitar a aplicação e adaptação.

2 CÓDIGOS, CIFRAS E CRIPTOGRAFIA

Visto que a presença dos códigos é muito marcante no cotidiano das pessoas, o objetivo desse capítulo é dar mais evidência a essa participação tanto na atualidade quanto através dos tempos por meio de fatos históricos que também objetivam despertar a curiosidade e o interesse por uma proposta baseada no tema.

Outro campo amplamente rico para a matemática é a criptografia. Embora seu foco não seja o objeto deste trabalho, o leitor poderá perceber que em muitos casos os códigos, cifras e criptografia estão intimamente interligados tornando difícil e enfadonho tratar de apenas um destes isoladamente. Tanto pelo interesse histórico, quanto pela curiosidade, abordaremos aqui, inicialmente os três conceitos. Contudo é importante deixar claro que não se tratam da mesma coisa. Segundo Couto (2008), o código dá uma forma diferente aos dados analisados afim de torná-los mais apropriados para uma determinada aplicação. Já as cifras são um conjunto de regras que permitem que a mensagem seja codificada e posteriormente decodificada a fim de torná-la ininteligível para um interceptador.

A palavra grega *kryptos* é usada para descrever algo oculto, escondido, enquanto que *graphos* está relacionada à escrita. Outras palavras que se relacionam a essas são *logos* (estudo, ciência) e *analysis*, (decomposição). E assim a criptologia é o estudo da escrita cifrada ocupando-se da criptografia, estudo das técnicas utilizadas para escrever uma mensagem ilegível para outrem que não seus remetentes e destinatários, e criptoanálise. Sendo esta o estudo das formas de ler as mensagens cifradas.

Pode parecer que o estudo de códigos ou a criptologia sejam desprovidos de valor e utilidade prática, mas ao usar um celular, por exemplo, sua voz é codificada em impulsos eletromagnéticos, transmitida e decodificada novamente para que a outra pessoa seja capaz de compreendê-la. Algo semelhante acontece com o rádio, a TV e até no computador, onde as informações digitadas são convertidas em linguagem binária para só então serem processadas. Mais do que transmitir mensagens, tais processos permitem a realização de transações eletrônicas como as, cada vez mais frequentes, compras pela internet e o sigilo dos seus dados na transmissão de mensagens por e-mail.

2.1 Os Hieróglifos

Enganam-se também aqueles que acreditam que cifras e códigos são especificidades da Idade Contemporânea:

> É mesmo na história da humanidade, mais precisamente em seus primórdios, que temos que procurar pelas origens não reveladas da arte da

> codificação. Um exemplo de código muito conhecido do grande público é a decifração dos famosos hieróglifos no Antigo Egito. Era uma linguagem que poucos cidadãos conheciam e que, mesmo assim, carregava um ar místico para os lugares onde era esculpida. (COUTO, 2008, p. 4).

Eves (2011, p. 67) afirma que durante muito tempo o Egito foi o mais rico campo de pesquisas sobre a Antiguidade graças à veneração que os egípcios tinham pelos seus mortos, que levou à construção de tumbas e templos perenes com ricas inscrições em suas paredes, e ao clima seco da região que permitiu a preservação de muitos papiros que teriam desaparecido de outra forma.

E é desse contexto de mistério que advém muito do fascínio pelos hieróglifos. O termo é formado pela junção de duas palavras gregas, *hieros* (sagrado) e *glyphós* (escrita). Eram usados exclusivamente pelas camadas mais altas da sociedade egípcia como sacerdotes, membros da realeza e, claro, escribas.

Além de ser considerado pelos egiptólogos uma linguagem difícil, fatores como invasão de vários povos ao longo da história e principalmente a introdução das línguas grega e romana, bem como a conquista por esses impérios contribuíram para o esquecimento da antiga linguagem. Outro fato importante foi o preconceito que os hieróglifos sofreram dos primeiros cristãos pelo fato de ser uma escrita "sagrada" relacionada, para os cristãos, ao paganismo e portanto proibida. O fato é que por essas razões muito do passado da civilização egípcia caiu no esquecimento. Coube ao francês Jean-François Champollion (1790-1832) decifrar a escrita egípcia antiga. Porém, o caminho até a realização desse feito foi longo e árduo. E um fator decisivo foi o achado da Pedra de Rosetta por uma expedição de Napoleão ao Egito em 1799. Segundo Eves (2011, p. 70-71), a pedra foi gravada em 196 a.C., mede 109 cm de altura por 76 cm de largura e contém inscrições com uma mensagem repetida em hieróglifos, demótico (forma simplificada de escrita egípcia) e grego.

Tomando o grego como base e expandindo os trabalhos de Thomas Young, Champollion foi capaz de "quebrar" o código egípcio.

Além dos egípcios, outras civilizações também usaram de alguma maneira cifras e códigos, principalmente em guerras. Uma das mais famosas é a Cifra de César.

> [...] a criptografia é uma ciência antiga e somente nos dias modernos passou a ser uma atividade controlada e dirigida para alguma finalidade acadêmica. Antes disso, todos possuíam certos códigos que eram usados em ocasiões especiais, seja para proteger segredos militares ou comerciais, mas a maneira como foram usados era completamente informal. Então não é de se espantar que tenhamos encontrado uma mensagem criptografada num tablete da Mesopotâmia, por exemplo. (COUTO, 2008, p. 15).

2.2 Códigos de Guerra

"[...] praticamente não houve uma guerra em que não houvesse por perto especialistas em cifras e códigos. A maioria deles estudava o assunto e alguns simplesmente nasciam com o dom. " (COUTO, 2008, p. 259).

Como já foi dito, a Cifra de César é uma das mais conhecidas e se baseia no deslocamento de letras. César deslocava três posições, ou seja, cada letra da mensagem original era substituída pela terceira seguinte do alfabeto, como pode ser visto no quadro 1.

Quadro 1 – Cifra de César.

Alfabeto Normal	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Com Deslocamento	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Fonte: Couto (2008, p. 16).

Como exemplo, a "mensagem"

$$CIFRA\ DE\ CESAR$$

seria transformada em

$$FLIUD\ GH\ FHVDU$$

Embora não haja nenhum documento histórico que comprove a eficácia do método, provavelmente o sucesso do método, muito simples para os padrões modernos, fosse garantido pela ínfima quantidade de inimigos alfabetizados e pela improvável realização de uma criptoanálise por parte deles na mensagem cifrada.

Apesar da simplicidade, a Cifra de César continuou sendo usada com outros deslocamentos ou em conjunto com outros métodos de cifragem. Tanto é que, Couto (2008, p. 17), nos relata que em 1915, em plena Primeira Guerra Mundial, a cifra foi mais bem aproveitada pelas tropas russas do que outras mais complicadas. Só que de forma igualmente simples, criptoanalistas alemães e austríacos decifraram as mensagens.

Outro caso bastante interessante foi a utilização do Código Navarro durante a Segunda Guerra Mundial. Pois, apesar da existência de máquinas de criptografia, muitas delas apresentavam problemas, não eram apropriadas para uso em campo e mesmo quando apresentavam o resultado desejado demoravam muito para fazê-lo.

O exército norte americano conseguiu contornar esses problemas com o treinamento e participação na guerra dos nativos americanos. Utilizando a língua dos índios Navajo, foi compilado um dicionário que fazia correspondência entre termos do mundo natural e militar. Como exemplo, avião era chamado de andorinha e submarino de peixe (quadro 2). Também desenvolveram um alfabeto codificado nessa mesma língua para soletrar palavras

em situações imprevisíveis. O código, até onde se sabe, permaneceu impenetrável até o fim da guerra, mas sua existência só se tornou conhecida em 1968 ainda considerado de interesse para segurança nacional. Apenas em 1982 os Estados Unidos elegeram o dia 14 de agosto como o Dia Nacional dos Faladores de Código Navajo.

Quadro 2 – Código Navajo.

Palavra	Em Código	Tradução Navarro
Avião de guerra	Beija-flor	Da-he-tih-hi
Avião de observação	Coruja	Ne-as-jaqh
Avião	Andorinha	Tas-chizzie
Avião bombardeiro	Falcão	Jay-sho
Bombardeiro mergulhador	Búteo-de-cauda-vermelha	Gini
Bombas	Ovos	A-ye-shi
Veículo anfíbio	Sapo	Chal
Couraçado	Baleia	Lo-tso
Destroyer	Tubarão	Ca-lo
Submarino	Peixe	Besh-lo

Fonte: Couto (2008, p. 151).

Ainda na Segunda Guerra Mundial, um caso bastante chamativo foi o da máquina de criptografia Enigma, que se assemelhava a uma máquina de escrever, adotada pelos nazistas e também por outros governos. Alguns historiadores afirmam que decifrar esse código pode ter antecipado o fim da guerra em até um ano.

Talvez o que torne sua história ainda mais interessante seja o fato de ter sido patenteada em 1918 por Arthur Scherbius, comercializada livremente a partir de 1923 e só ter sido retirada de circulação quando o exército alemão percebeu sua utilidade e adotou versões melhoradas da mesma.

A obtenção de um modelo pelos aliados e a contribuição inicial dos poloneses foram cruciais para decifrar o código alemão. Dada a dificuldade da tarefa, até o formalismo exagerado das mensagens alemãs foi de utilidade para tentar desvendar o padrão de codificação das máquinas. Foram os poloneses os primeiros a criarem máquinas eletromecânicas, conhecidas como "bombas" para reconstrução das chaves diárias usadas pelos nazistas na cifragem de suas mensagens. Mas foi com os desenvolvimentos do matemático britânico Alan Turing (1912-1954) que o processo de decodificação das máquinas Enigma foi realmente acelerado e permitiu o desenvolvimento de novas "bombas" capazes de quebrar o código nazista.

Um pouco da história de Alan Turing e seu trabalho para decodificar a máquina Enigma são retratados no filme "O Jogo da Imitação" (The Imitation Game no original em inglês) de 2014.

2.3 Um Mundo Fascinante

Como deve ter ficado claro, o mundo das cifras e dos códigos se entrelaça de tal modo que alguns chegam a pensar que são sinônimos. Mais do que utilidade bélica no entanto, muitos códigos foram criados para contornar várias dificuldades da interação humana, como o sistema de leitura para cegos inventado pelo francês Louis Braille em 1929. Outros, simplesmente despertam a curiosidade e continuam misteriosos através dos séculos.

Nos capítulos seguintes será dada enfase ao código de barras e a uma de suas evoluções bidimensionais cujo propósito de criação está ligada à automação de processos nas empresas e expandiu-se para uma gama variadíssima de utilidades principalmente após o advento dos smartphones, cada vez mais potentes.

Outro código, bastante famoso, é o código Morse. Ele foi criado em 1835, por Samuel Morse e Alfred Vail, e utilizado no telégrafo elétrico. Uma mensagem nesse código pode ser transmitida em vários ambientes diferentes por pulsos curtos e longos como:

- pulsos elétricos transmitidos por um cabo;
- ondas mecânicas ou perturbações sonoras;
- sinais visuais (luzes ascendendo e apagando);
- ondas eletromagnéticas (sinais de rádio);

Internacionalmente, o código Morse é composto por seis elementos:

1. Sinal curto, ponto ou “dit” (.);
2. Sinal longo, traço ou “dah” (-);
3. Intervalo entre caracteres (entre pontos e traços);
4. Intervalo curto (entre letras);
5. Intervalo médio (entre palavras);
6. Intervalo longo (entre frases);

O quadro 3 apresenta letras e números no código Morse Internacional de acordo com SOS (2016).

Uma importante aplicação do código Morse é a sinalização para obtenção de ajuda através do SOS. O sinal foi adotado internacionalmente a partir de 1906 tendo sido descontinuado oficialmente só em 1º de janeiro de 1998. Ao invés de letras, é apenas um

Quadro 3 – Código Morse Internacional.

Letra	Código Internacional	Letra	Código Internacional	Let/Num	Código Internacional
A	. -	M	- -	Y	- . - -
B	- . . .	N	- .	Z	– . .
C	- . - .	O	- - -	1	. - - - -
D	- . .	P	. - - .	2	. . - - -
E	.	Q	- - . -	3	. . . - -
F	. . - .	R	. - .	4	. . . . -
G	- - .	S	. . .	5	. . . . .
H	. . . .	T	-	6	- . . . .
I	. .	U	. . -	7	- - . . .
J	. - - -	V	. . . -	8	- - - . .
K	- . -	W	. - -	9	- - - - .
L	. - . .	X	- . . -	0	- - - - -

Fonte: https://en.wikipedia.org/wiki/Morse_code.

grupo de pontos e traços (. . . - - - . . .) escolhido por ser um padrão gráfico bastante simples e inconfundível. Como pode ser decodificado por "SOS", a palavra ainda hoje é reconhecida como um sinal de emergência.

Com o aparecimento de tecnologias mais avançadas o código Morse se tornou obsoleto, mas ainda é usado, principalmente no radio amadorismo, e considerado um modo de modulação facilmente compreendido por seres humanos sem ajuda de aparelhos mais sofisticados. No entanto, o comprimento variável dos seus caracteres dificulta a adaptação em meios de comunicação automatizados e por isso foi amplamente substituído por formatos regulares como o código ASCII, comum em computadores.

Por outro lado, alguns códigos antigos permanecem incompreensíveis até hoje. Entre eles está o manuscrito Voynich que é um livro com mais de duzentas páginas e ricamente ilustrado com plantas, estrelas e figuras humanas. Especialistas acreditam ser datado do século XV. O fato é que, desde que o manuscrito foi encontrado, despertou a atenção de muitos estudiosos e mesmo criptógrafos renomados não conseguiram decifrá-lo.

Alguns acreditam que o manuscrito não passa de uma farsa ou que não tem sentido algum. Porém, pesquisadores contra-argumentam essa hipótese com base em técnicas estatísticas que indicam que fatores apresentados no texto são característicos de uma linguagem cifrada e não de uma sequência de símbolos sem sentido.

Também entre os grandes enigmas criptográficos não resolvidos estão as cifras de Beale. São três textos cifrados que supostamente indicam a localização de um tesouro avaliado em dezenas de milhões de dólares. Cada uma das cartas é composta somente de uma sequência de números separados por vírgulas, mas apenas a segunda foi decifrada

(figura 2.1)usando como chave o documento de Declaração de Independência dos Estados Unidos da América.

Por mais estranho que possa parecer, qualquer um pode pegar uma cópia do documento da declaração de Independência, numerar suas palavras e seguir a ordem indicada pelos números da segunda carta obtendo a descrição do tesouro através da inicial da palavra correspondente. Entretanto, toda a história em torno dos textos parece apontar para uma farsa bem elaborada, como o fato de somente a carta dois (descrição do tesouro) ter sido quebrada atraindo a atenção para os demais textos. Criptógrafos também alegam que as cartas restantes possuem características estatísticas que sugerem não haver qualquer texto cifrado em inglês, o que não impediu muitos outros de tentarem "quebrar" os textos ou procurar outros documentos históricos como chave para as cartas restantes.

Figura 2.1 – Segunda Carta de Beale - Única decifrada.

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

Fonte: https://pt.wikipedia.org/wiki/Cifras_de_Beale.

2.4 Uma Cifra Interessante

Apesar da matemática permear o campo dos códigos, das cifras e da criptografia, muitos conteúdos podem ser demasiadamente complexos para alunos da educação básica. Cabe ao professor explorar os aspectos históricos dos temas e dosar o conteúdo matemático

corretamente por meio de adaptações em atividades ou escolha de exemplos que não tornem o processo enfadonho e complicado demais, gerando um efeito oposto ao que se pretende.

Segundo Couto (2008, p. 115), um bom meio de entender a criptografia moderna sem ter que enfrentar a teoria dos números e matemática próprias dessa ciência é a Cifra Playfair, inventada pelo cientista Charles Wheatstone em 1854. Após sua invenção o Barão Lyon Playfair, amigo de Wheatstone, conseguiu que o governo britânico adotasse oficialmente o uso da cifra e daí o nome Cifra Playfair.

Apesar de ser considerada de baixa segurança, essa cifra possui algumas vantagens como não precisar de tabelas ou dispositivos complicados, possuir uma palavra chave que pode ser memorizada ou trocada com facilidade, ser de fácil implementação e pouco sujeita a erros. Essas características a tornam uma excelente cifra de campo.

Para ilustrar, vamos cifrar a mensagem "DOIS É O PRIMEIRO NÚMERO PRIMO". O primeiro passo é organizar a mensagem em blocos de duas letras desconsiderando acentos e espaços:

$$DO\ IS\ EO\ PR\ IM\ EI\ RO\ NU\ ME\ RO\ PR\ IM\ O$$

Não pode haver blocos com letras repetidas nem blocos com apenas uma letra. Quando isso ocorre substituímos a segunda letra por uma outra que foi convencionada como X ou Z. Caso falte uma letra no final, também adicionamos X ou Z:

$$DO\ IS\ EO\ PR\ IM\ EI\ RO\ NU\ ME\ RO\ PR\ IM\ OX$$

Agora podemos definir a "chave" para o nosso alfabeto cifrante. Wheatstone propôs que a palavra-chave ficasse disposta em uma grade de cinco linhas por cinco colunas. Como nosso alfabeto possui 26 letras será preciso eliminar uma delas. Aqui, vamos eliminar o W substituindo-o por V. Para facilitar o entendimento, preencheremos a grade com a palavra-chave PLAYFAIR no início e completamos os demais espaços com o alfabeto em ordem alfabética. Caso alguma letra se repita (caso do A) ela é suprimida nas próximas ocorrências. A grade ficará como mostrado no quadro 4.

As letras de um bloco só podem assumir três posições na grade: estão na mesma linha, estão na mesma coluna ou estão em linhas e colunas diferentes. Assim, para fazer as substituições basta seguir três regras:

a) Letras na mesma linha - são substituídas pelas letras imediatamente a sua direita. Caso uma das letras esteja na última coluna da grade, "reiniciamos" a linha e pegamos a letra da primeira coluna.

Quadro 4 – Grade Cifrante.

P	L	A	Y	F
I	R	B	C	D
E	G	H	J	K
M	N	O	Q	S
T	U	V	X	Z

Fonte: feito pelo autor.

b) Letras na mesma coluna - são substituídas pelas letras imediatamente abaixo delas. Caso umas das letras esteja na última linha, pegamos a primeira letra da coluna.

c) Letras em linhas e colunas diferentes - as letras do bigrama formarão um "quadrilátero" e serão substituídas pelas letras dos cantos opostos na mesma linha. Mas a ordem é importante - a primeira letra do par cifrada será correspondente àquela que se encontra na mesma linha da primeira letra do par de texto simples.

O primeiro par de letras (bloco bigrâmico), *DO*, se encontra em linhas e colunas diferentes. Logo, o *D* e o *O* formarão um quadrilátero conforme o quadro 5. Assim, o nosso bloco bigrâmico cifrado deve ser *BS*, pois o *D* é a primeira letra do nosso bloco e o *B* é a "letra de canto" que se encontra na mesma linha que ele. Da mesma forma, o *O* é a segunda letra e o *S* é a "letra de canto" que se encontra na mesma linha que ele.

Quadro 5 – Quadrilátero DO.

B	C	**D**
H	J	K
O	Q	S

Fonte: feito pelo autor.

Já as letras do bloco *IM*, encontram-se na mesma coluna. O *I* é a primeira letra e dever ser substituído por *E* que se encontra imediatamente abaixo dela. Analogamente, a segunda letra, *M*, será substituída por T completando o bloco cifrado *ET*

Obedecendo às regras nos demais blocos bigrâmicos, teremos a mensagem cifrada conforme o quadro 6. Para decifrar, basta fazer o processo inverso nas três regras e desconsiderar as letras que não façam sentido (caso do V, X ou Z) conforme a convenção estabelecida entre as partes.

Relembramos que, embora o foco do trabalho esteja em códigos, a Cifra Playfair, como o próprio nome indica, é um exemplo de cifra relacionando-se mais à criptografia, pois o seu objetivo é tornar a mensagem ilegível para aqueles que não fazem parte desse processo de comunicação e não dispõem da "chave" para decifrar a mensagem.

Quadro 6 – Mensagem Cifrada.

DO	IS	EO	PR	IM	EI	RO	NU	ME	RO	PR	IM	OX
BS	DM	HM	LI	ET	ME	BN	UL	TM	BN	LI	ET	QV

Fonte: feito pelo autor.

3 CÓDIGO DE BARRAS

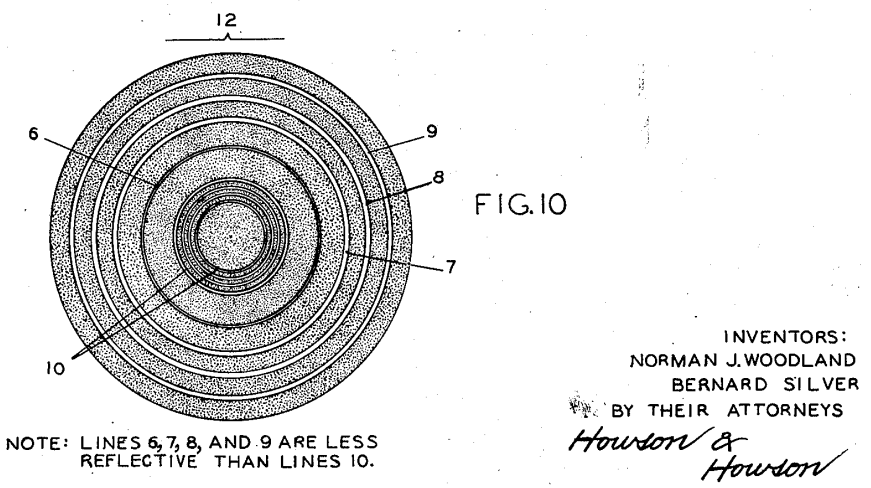
Neste capítulo apresentamos um breve relato da criação dos códigos de barras por Joseph Woodland e Bernard Silver e seu objetivo de transformar tarefas como o fechamento de contas de supermercados em algo mais rápido e simples. Porém, apesar da infinidade de tipos de códigos de barras e da praticidade gerada por eles, sua adoção definitiva só ocorreu muitos anos após seu surgimento.

Destacamos as duas versões mais comuns dos códigos de barras que são justamente aquelas encontradas em produtos de supermercados: o código UPC-A e o EAN-13. Vemos como ler tais códigos e como uma mera diferenciação de paridade na codificação dos números permite tanto a ampliação do código quanto sua leitura de cabeça para baixo. Enquanto o UPC-A é adotado nos Estados Unidos e Canadá, o EAN-13 surgiu como uma ampliação devido à necessidade de expansão internacional do código. Fato que pode ser evidenciado pela presença de um campo, dentre outros, para identificação do país de registro do produto na estrutura do código de barras.

3.1 A Origem do Código de Barras

Uma primeira versão de um código de barras foi registrada em 20 de outubro de 1949 pelos inventores Joseph Woodland e Bernard Silver. Mas, como pode ser visto na figura 3.1, esse código não se assemelhava com as barras verticais que conhecemos hoje. Foi chamado de “Bulls Eye” (olho de boi) e era formado por círculos concêntricos de espessuras variáveis.

Figura 3.1 – Bulls Eye.



Fonte: http://www.google.com/patents/US2612994.

Em 1948 o dono de uma rede de supermercados, com o intuito de agilizar o processo de cálculo das contas dos clientes no momento da saída da loja, solicitou ao Instituto de Tecnologia Drexel (atual Universidade Drexel), na Filadélfia uma forma de ler o produto no caixa. Bernard Silver se juntou a outro estudante do instituto, Joseph Woodland, para trabalharem em uma solução a essa solicitação.

A primeira ideia foi trabalhar com uma tinta especial sensível à luz ultravioleta, porém, apesar de funcionar, havia problemas com a instabilidade da tinta e custos elevados para as impressões. Supostamente em 1949, de férias em uma praia de Miami, Woodland teve uma ideia para resolver o problema ao observar as marcas de linhas feitas por seus dedos na areia e perceber que poderia representar algo com linhas de espessuras diferentes em uma espécie de código Morse visual.

Finalmente, em 7 de outubro de 1952, a patente foi emitida e seus direitos foram vendidos para a Philco. Porém, a empresa não obteve lucros com ela, visto que a primeira aplicação comercial ocorreu somente em 1974, anos após o vencimento dos direitos sobre a patente.

Em 1970, George Laurer, da IBM, criou um código aceito formalmente em 1973 que passou a ser conhecido como UPC - Universal Product Code (Código Universal de Produto) adotado nos Estados Unidos e Canadá. A primeira leitura desse tipo de código ocorreu em uma manhã de 26 de junho de 1974, quando Clyde Dawson comprou um pacote de chicletes em um supermercado da cidade de Troy, Ohio, Estados Unidos. Existem hoje, variados tipos de códigos de barras. Entre eles está o EAN (European Article Numbering System) que foi uma ampliação para permitir a difusão do sistema de modo a identificar também o país de origem do produto classificado. Acabou sendo criado um novo código de 13 dígitos compatível com os leitores do código UPC.

3.2 Como Funciona o Código de Barras

Apesar de alguns tipos específicos de códigos de barras e versões para casos especiais como caixas pequenas, por exemplo, podemos identificar dois principais que são o UPC-A adotado nos Estados Unidos e Canadá e o EAN-13 adotado na Europa e internacionalmente.

Visualmente é fácil perceber que existem diferenças nas espessuras das listras. Na verdade, essa impressão é causada pela justaposição de listras de uma mesma cor. No entanto, para facilitar nossa compreensão, podemos separá-las em quatro tipos quanto a sua espessura: fina, média, grossa e muito grossa. Cada tipo de listra receberá um símbolo para identificá-la de acordo com sua espessura e cor conforme o quadro 7.

Cada espaço de espessura fixa no código de barras corresponde exatamente a uma sequência de sete dígitos iguais a 0 ou 1 e cada sequência corresponde a um número. Na

Figura 3.2 – Código UPC-A.

Fonte: http://www.ebah.com.br/content/ABAAAfOyYAJ/codigos-barra.

Quadro 7 – Codificação das Listras.

Listra	Branca	Preta
Fina	0	1
Média	00	11
Grossa	000	111
Muito Grossa	0000	1111

Fonte: feito pelo autor.

figura 3.2, deixando de lado as três primeiras listras finas e mais compridas (preta, branca e preta) que servem de limitação, podemos observar a primeira sequência formada por listras branca média, preta média, branca média e preta fina. Fazendo a correspondência pelo quadro 7 temos a sequência binária 0011001 que corresponde ao número 1. Antes de prosseguir é importante ressaltar que os números que aparecem abaixo do código de barras não estão necessariamente em correspondência com as barras que os representam e que os números são codificados de maneiras diferentes quando estão do lado esquerdo ou direito do código de barras.

No quadro 8, vemos que os números da coluna da direita são obtidos trocando-se cada 0 dos números da coluna da esquerda por 1 e vice-versa. Atente também para o fato de que cada número da coluna da esquerda tem uma quantidade ímpar de dígitos iguais a 1 e consequentemente, pela forma como são obtidos, os números da coluna da direita tem uma quantidade par. Essa diferenciação permite que a máquina identifique se o código está sendo lido de cabeça para baixo ou não. Para fixação das ideias vamos "ler" o código de barras anteriormente apresentado com a ajuda do quadro 8 e da distinção dos setores através de cores.

Quadro 8 – Codificação de Dígitos.

Dígito	Lado Esquerdo	Lado Direito
0	0001101	1110010
1	0011001	1100110
2	0010011	1101100
3	0111101	1000010
4	0100011	1011100
5	0110001	1001110
6	0101111	1010000
7	0111011	1000100
8	0110111	1001000
9	0001011	1110100

Fonte: https://pt.wikipedia.org/wiki/Código_de_barras.

Figura 3.3 – Código Dividido por Setores.

Fonte: http://www.ebah.com.br/content/ABAAAfOyYAJ/codigos-barra - modificado pelo autor.

1. As três primeiras barras na parte roxa da figura 3.3 são barras limitadoras e sempre representadas por **preta fina** – **branca fina** – **preta fina** (101);
2. Em seguida temos **branca média** – **preta média** – **branca média** – **preta fina** (0011001) que equivale a 1;
3. No terceiro setor, pintado de cinza, identificamos **branca fina** – **preta muito grossa** – **branca fina** – **preta fina** (0111101) que equivale a 3;
4. 0110111 – 8;
5. 0001101 – 0;
6. 0110001 – 5;

7. 0110001 – 5;
8. O oitavo setor em roxo no centro do código são cinco barras finas sempre representadas por 01010 e dividem o código em lado esquerdo e direito. A partir desse ponto os números passam a ser codificados de acordo com a coluna da direita do quadro 8;
9. 1010000 – 6;
10. 1001110 – 5;
11. 1100110 – 1;
12. 1001110 – 5;
13. 1011100 – 4;
14. 1000100 – 7;
15. E finalmente as três últimas barras limitadoras (sempre 101).

Como visto anteriormente, o EAN surgiu da necessidade de se adicionar mais um dígito ao código de forma a permitir a identificação do país de origem do produto. Porém isso devia ser feito mantendo o mesmo padrão de tamanho nos códigos para que as máquinas pudessem ler indistintamente códigos UPC e EAN. Assim, os países que utilizavam o código UPC antigo, Estados Unidos e Canadá, são identificados com um 0 na frente e o resto da codificação é feito como visto acima.

Para os demais países o novo dígito aparece implicitamente de acordo com o padrão com que os números do lado direito do código são escritos. Um dígito do lado esquerdo pode agora ser escrito com quantidade ímpar ou par de dígitos iguais a 1 dependendo da posição em que aparece. O quadro 9 mostra a paridade de codificação de cada dígito:

A paridade que a codificação de cada número deve assumir dependerá do primeiro dígito do código de barras. O quadro 10 mostra a alternância entre pares e ímpares referente ao primeiro dígito do código.

Para exemplificar, utilizaremos o código de barras EAN-13 da figura 3.4.

Observe que o primeiro dígito é 7, logo ele deve aparecer, implicitamente, na codificação dos demais e consequentemente a ordem de codificação será **ímpar – par – ímpar – par – ímpar – par**, de acordo com o quadro 10. Consultando-se o quadro de codificação EAN-13 tem-se:

1. Barras limitadoras à esquerda (sempre as mesmas): **101**;
2. Lado esquerdo, codificação de paridade ímpar (5): **0110001**;

Quadro 9 – Codificação EAN-13.

Dígito	Codificação do Lado Esquerdo		Codificação do Lado Direito
	Paridade Ímpar	Paridade Par	Paridade Inalterada
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
0	0001011	0010111	1110100

Fonte: barcodeisland.com/ean13.phtml.

Quadro 10 – Distribuição de Paridade.

Dígito Inicial	Paridade dos Seis Dígitos do Lado Esquerdo					
0 (UPC-A)	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar
1	Ímpar	Ímpar	Par	Ímpar	Par	Par
2	Ímpar	Ímpar	Par	Par	Ímpar	Par
3	Ímpar	Ímpar	Par	Par	Par	Ímpar
4	Ímpar	Par	Ímpar	Ímpar	Par	Par
5	Ímpar	Par	Par	Ímpar	Ímpar	Par
6	Ímpar	Par	Par	Par	Ímpar	Ímpar
7	Ímpar	Par	Ímpar	Par	Ímpar	Par
8	Ímpar	Par	Ímpar	Par	Par	Ímpar
9	Ímpar	Par	Par	Ímpar	Par	Ímpar

Fonte: barcodeisland.com/ean13.phtml.

3. Lado esquerdo codificação de paridade par (0): **0100111**;
4. Lado esquerdo codificação de paridade ímpar (1): **0011001**;
5. Lado esquerdo codificação de paridade par (0): **0100111**;
6. Lado esquerdo codificação de paridade ímpar (3): **0111101**;
7. Lado esquerdo codificação de paridade par (1): **0110011**;
8. Barras centrais (sempre as mesmas): **01010**;
9. Lado direito, codificação padrão (3): **1000010**;
10. Lado direito, codificação padrão (1): **1100110**;

Figura 3.4 – Codificação EAN-13.

Fonte: http://www.barcodeisland.com/ean13.phtml.

11. Lado direito, codificação padrão (1): **1100110**;
12. Lado direito, codificação padrão (3): **1000010**;
13. Lado direito, codificação padrão (0): **1110010**;
14. Lado direito, codificação padrão (9): **1110100**;
15. Barras limitadoras à direita (sempre as mesmas): **101**.

3.3 Estrutura do Código de Barras

Os números que aparecem no código de barras não são simplesmente aleatórios. No caso do EAN-13, composto por 13 números, temos a identificação do país, identificação do fabricante, identificação do produto e um dígito de controle.

- Identificação do país - os dois ou três primeiros números, dependendo do caso, indicam o país[1] onde o produto foi cadastrado e não necessariamente onde ele foi fabricado. No caso do Brasil esse número é 789;
- Identificação do fabricante - os próximos quatro ou sete números representam a empresa detentora do código de barras. Esse número é fornecido pela EAN;
- Identificação do produto - o próximo grupo de dígitos representa a identificação do produto na empresa. São atribuídos pelo próprio fabricante desde que sejam únicos para cada produto. Como a maioria das empresas não terá uma quantidade muito grande de produtos, é possível deixar menos dígitos para identificá-los e assim fazer um melhor uso do código.

[1] Uma tabela com os dígitos verificadores de cada país pode ser encontrada em http://www.barcodeisland.com/ean13.phtml

- Dígito verificador - o último dígito do código é usado para verificar se o código foi digitado ou escaneado corretamente e é calculado com base nos demais dígitos do código de barras. Mais detalhes serão apresentados no capítulo 5.

Na figura 3.5 estão presentes três códigos de barras que permitem fazer algumas observações acerca de sua estrutura. As inscrições apresentadas na embalagem do primeiro código (8023277101326) dão a impressão de ser um produto de origem italiana. Impressão, essa, confirmada pelos dígitos iniciais do código, pois a Itália é identificada pelos números de 80 a 83. Já os outros dois códigos pertencem a produtos de uma famosa empresa nacional de cosméticos. Além da identificação do país (Brasil 789), também é possível identificar quais dígitos representam a marca da empresa e quais representam o produto. Por se tratarem de produtos de uma mesma empresa, espera-se, evidentemente, que o segundo grupo de dígitos seja o mesmo. Logo, podemos inferir que essa empresa é representada por 9563 nos códigos de barras, sendo que os cinco algarismos seguintes são para identificação dos seus produtos (82030 e 21034 respectivamente). O último dígito só pode ser de verificação e depende justamente dos demais.

Figura 3.5 – Estrutura do EAN-13.

Fonte: feito pelo autor.

Já na figura 3.6, temos códigos de marcas de refrigerante famosas. Apesar de serem produtos similares, não encontramos nada em comum além do país de registro entre marcas diferentes. O que já era esperado, visto que a codificação do produto é atribuída pelo próprio fabricante. Especialmente no segundo e terceiro código temos o mesmo produto, porém o fato de serem vendidos em embalagens diferentes já ocasiona uma modificação em seus códigos de barras.

Figura 3.6 – EAN-13 de Produtos Similares.

Fonte: feito pelo autor.

4 QR CODE

No presente capítulo, abordamos o surgimento do QR code e seu intuito de facilitar processos em linhas de montagem por meio da substituição de vários códigos de barras, além da possibilidade de representação de mais conteúdos, personalização e resistência a danos e erros. Também apresentamos os pontos mais característicos da estrutura de um QR code e a leitura de um modelo. Em virtude da clara dificuldade de criação e leitura manual de tais códigos, apresentamos indicações de aplicativos e sites para a execução dessas tarefas juntamente com alguns exemplos. Ainda neste capítulo, podem ser encontrados comentários e imagens de alguns outros códigos bidimensionais.

4.1 A Origem do QR Code

O código QR ou QR code (Quick Response Code – Código de Resposta Rápida), é um código de barras bidimensional e pode ser facilmente escaneado pela maioria dos smartphones modernos. O código foi criado por uma empresa japonesa subsidiária da Toyota, a Denso-Wave, em 1994. A ideia era colocar mais informações em uma etiqueta menor substituindo vários códigos de barras por um código mais compacto, facilitando o rastreamento de partes e peças de carros na linha de montagem.

Até 7089 caracteres numéricos podem ser codificados em um único símbolo. Além disso, os QR Codes ainda são capazes de trabalhar com diversos tipos de dados como alfabéticos, kanji, kana, hiragana, binários, símbolos e códigos de controles. Também podem apresentar cores diferentes do clássico preto e branco e imagens no centro, além de serem resistente a certos tipos de danos e poderem ser lidos até de cabeça para baixo.

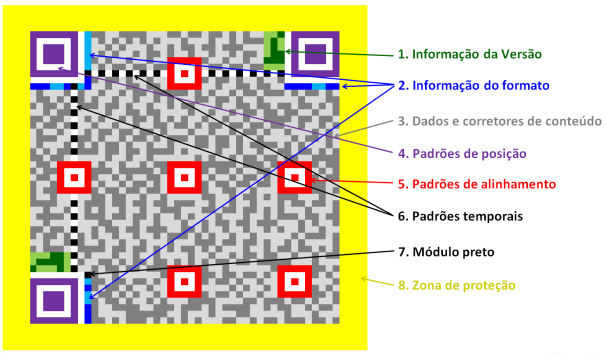
4.2 Como Funciona o QR Code

Embora haja variantes do QR code como o Micro QR Code ou iQR Code, as variações mais comuns quando nos referimos ao QR Code são os Model 1 e 2. Uma das características mais marcantes do código QR é sua forma quadrada subdividida em quadradinhos chamados módulos.

Existem quarenta versões do QR Code sendo que a versão 1, a menor, tem 21x21 módulos, a versão 2 tem 25x25 módulos e assim sucessivamente até a versão 40 que é composta por 177x177 módulos. Os módulos em um código QR podem ser agrupados em componentes distintos conforme a figura 4.1:

1. **Version information** - Esse campo informa a versão usada e só aparece da versão

Figura 4.1 – Estrutura do QR Code.



Fonte: feito pelo autor.

7 em diante. É colocado em dois lugares, em retângulos 6x3. Economiza tempo para se obter a informação da versão utilizada;

2. **Informação do formato** - Aqui são encontradas informações sobre o nível de correção de erro e a máscara de codificação usada. Dada a importância da leitura correta dessas informações, elas estão duplicadas e sempre são colocadas, independentemente da versão, ao lado dos padrões de posição;

3. **Dados e corretores de conteúdo** - É a mensagem propriamente dita juntamente com os campos de correção de erro.

4. **Padrões de posição** - Servem de orientação. Mostrando a posição do código e seus cantos. Seu tamanho é sempre 7x7;

5. **Padrões de alinhamento** - Mais um orientador de posição que serve de referência para leitura do código. Sua quantidade varia com o tamanho do símbolo, mas seu tamanho é fixo em 5x5;

6. **Padrões temporais** - Essas linhas auxiliam na percepção do posicionamento das linhas e colunas e também ajudam a determinar a dimensão do símbolo;

7. **Módulo preto** - Um simples módulo preto sempre colocado nesta posição ao lado do padrão de alinhamento inferior esquerdo;

8. **Zona de proteção** - Observe que também há separadores entre os padrões de posição e o interior do código.

4.3 Lendo um QR Code

Antes de começar a leitura manual de um código QR qualquer, é preciso estar atento a algumas características. A título de ilustração vamos decodificar a informação

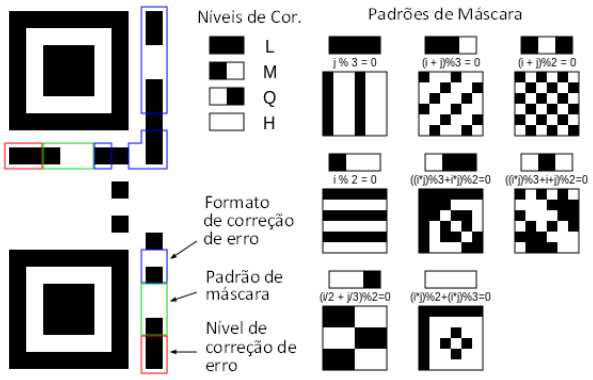
contida no símbolo a seguir (figura 4.2).

Figura 4.2 – QR Code para Decodificação.

Fonte: Código gerado pelo site http://mqr.kr.

O primeiro passo é descobrir qual "padrão de máscara" foi usado no código. O padrão de máscara é usado na codificação da mensagem para modificar setores que poderiam confundir o escâner, tais como muitos módulos brancos juntos ou setores que se pareçam com áreas reservadas. O padrão de máscara se repete como uma grade até cobrir todo o símbolo. As áreas correspondentes às partes escuras da máscara devem ter suas cores invertidas.

Figura 4.3 – Padrões de Máscara.



Fonte: https://en.wikipedia.org/wiki/QR_code[1].

Outra forma de descobrir quais módulos devem ter a cor invertida é por meio das fórmulas que aparecem na imagem que contém os padrões de máscara (figura 4.3). Suponha que as coordenadas do módulo na matriz do QR Code sejam $(3, 4)$ e quando substituídas na fórmula resultem em 0, então se o módulo for preto o lemos como branco e se for branco, lemos como se fosse preto.

[1] Traduzido pelo autor.

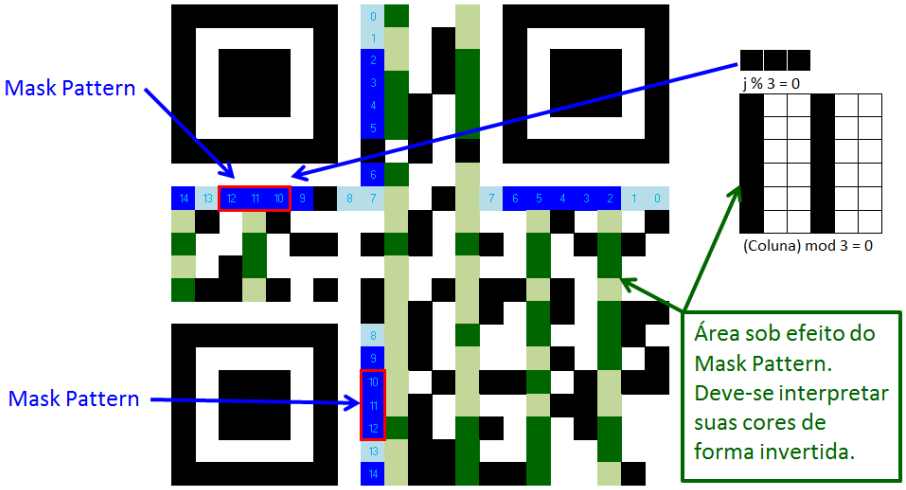
A simbologia apresentada nessas fórmulas remete à aritmética modular, mas podem ser facilmente compreendidas por meio de alguns exemplos:

- $(i+j)\%3 = 0$ corresponde a $(linha+coluna)\ mod\ 3 = 0$, que por sua vez significa que a soma dos números da linha e coluna na matriz deve ter resto igual a zero quando dividida por 3. Para um quadradinho de coordenadas $(3, 4)$ teríamos $(3+4)\ mod\ 3 = 1$ e consequentemente esse quadradinho não estaria sob influência da máscara;

- $(i/2+j/3)\%2 = 0$ corresponde a $(\lfloor linha/2 \rfloor + \lfloor coluna/3 \rfloor)\ mod\ 2 = 0$, onde a notação $\lfloor x \rfloor$ representa a função piso, que converte um número real x no maior número inteiro menor ou igual a x. Logo, a soma do maior inteiro igual ou inferior à divisão do número da linha por 2 com o maior inteiro igual ou inferior à divisão do número da coluna por 3 deve ter resto zero quando dividida por 2. Consequentemente, para o quadradinho de coordenadas $(3, 4)$ sob o efeito dessa máscara teríamos $(3/2 + 4/3)\%2 = (1 + 1)\%2 = 0$ e portando sua cor seria invertida.

Note que a contagem das linhas e colunas deve começar por 0. Também é importante perceber que o padrão de máscara afeta somente a área de dados e erro, não influenciando as partes reservadas do código (alinhamento, orientação, etc.). Levando em conta essas observações temos nosso código sob o efeito do padrão de máscara conforme a figura 4.4.

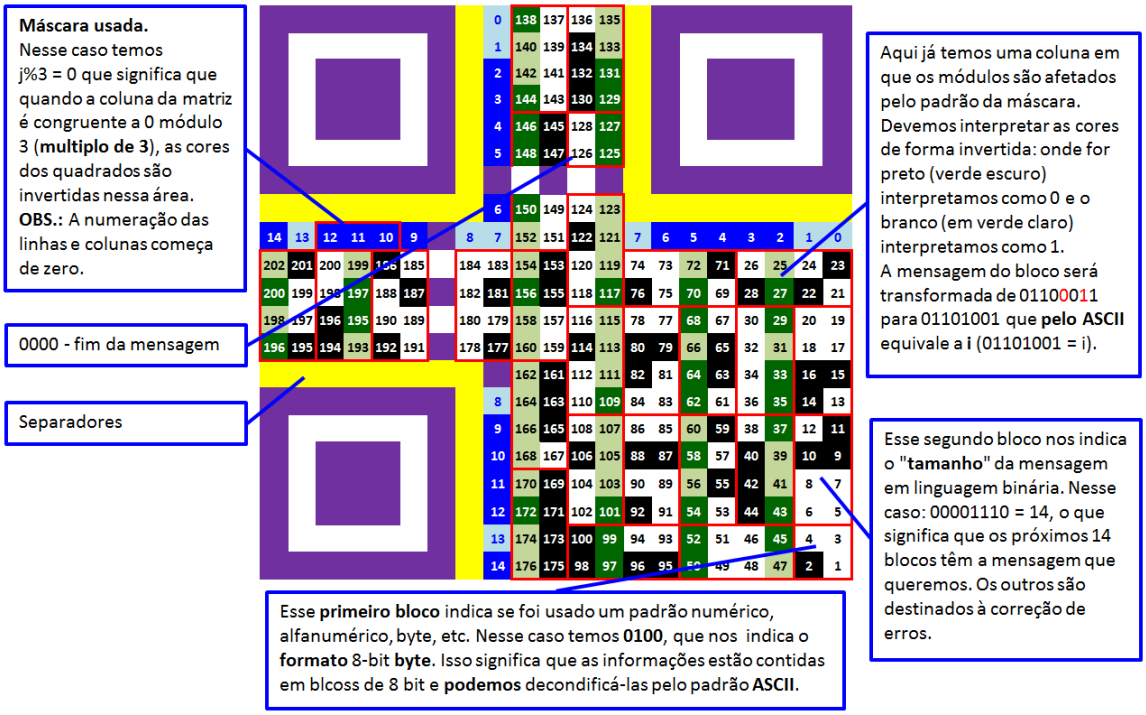
Figura 4.4 – Código Mascarado.



Fonte: feito pelo autor.

A leitura dos dados começa pelo primeiro módulo do canto inferior direito, passa para o primeiro a sua esquerda e volta para a coluna da direita uma linha acima e assim sucessivamente. Basicamente a leitura é feita em duas colunas (ou linhas) por vez em movimento de ziguezague. Na figura 4.5, os módulos serão numerados para facilitar a leitura na ordem correta.

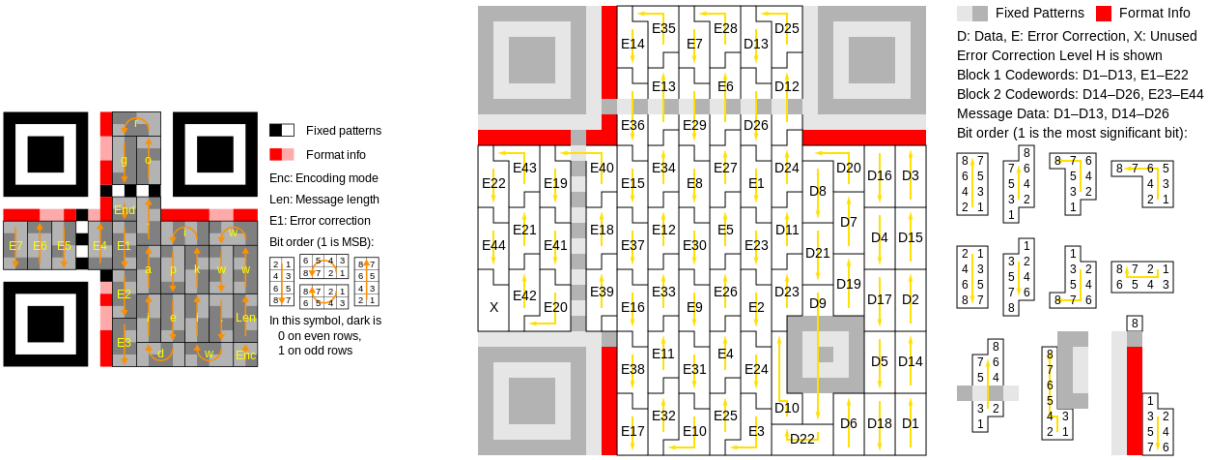
Figura 4.5 – Decodificando um QR Code.



Fonte: feito pelo autor.

Chegando ao topo, seguimos de forma a fazer com que a leitura volte ao sentido vertical nas próximas duas colunas. Os campos restritos às áreas de padrões fixos são ignorados e o formato que os "blocos de informação" assumem pode variar com a versão do símbolo e a forma de codificação. A figura 4.6 nos dá uma boa ideia dessa variação.

Figura 4.6 – Disposição da Informação.



Fonte: https://en.wikipedia.org/wiki/QR_code.

O primeiro bloco, formado por quatro módulos nos dá a informação sobre o tipo

de codificação do QR Code. No nosso exemplo, interpretando preto como 1 e branco como 0, os primeiros bits são 0100 que nos dizem que foi usado o modo "Byte" com 8 bits por caractere, que por sua vez pode ser interpretado pelo padrão ASCII[2]. Assim sendo, agruparemos a mensagem em blocos de 8 bits.

O próximo bloco nos informará o tamanho da mensagem. No exemplo temos 00001110 que é a expressão binária para 14. Isso significa que a verdadeira mensagem está contida nos próximos 14 blocos de informação que (usando a tabela ASCII) são:

1. **01110000** - p
2. **01101001** - i
3. **00100000** - (espaço)
4. **00111101** - = (igual)
5. **00100000** - (espaço)
6. **00110011** - 3
7. **00101100** - , (vírgula)
8. **00110001** - 1
9. **00110100** - 4
10. **00110001** - 1
11. **00110101** - 5
12. **00101110** - . (ponto)
13. **00101110** - . (ponto)
14. **00101110** - . (ponto).

Podemos então concluir que a mensagem contida em nosso exemplo é $pi = 3,1415...$ Veja também que após o último bloco há uma sequência de quatro bits iguais a zero para indicar o fim da mensagem ($0000 - fim\ da\ mensagem$). Os blocos restantes são para correção de erro.

Os blocos de erro têm tamanho de oito bits e usam o algorítimo de correção de erros Reed-Solomon[3] com quatro níveis de correção que podem ser de 7% para o mais

[2] A tabelela ASCII foi escolhida aqui por ser compatível com os padrões vigentes e ser de fácil acesso na internet

[3] Mais informações podem ser encontradas em https://en.wikipedia.org/wiki/Reed–Solomon_error_correction

baixo até 30% para o mais alto. Graças à correção de erros é possível criar QR codes artísticos que contem erros, mas ainda assim podem ser lidos tornando-os mais chamativos aos olhos, com colorações, logos ou outras características.

O modo de codificação pode assumir outras formas além do Byte (0100 - 8 bits por caractere). São elas:

- **Numérica** - representado por 0001 e usando 10 bit por 3 caracteres;
- **Alfanumérica** - representado por 0010 e usando 11 por bits por 2 caracteres;
- **Kanji** - representado por 1000 e usando 13 bits por caractere.

O modo numérico é para dígitos de 0 a 9. Já o modo alfanumérico pode representar além dos dígitos decimais de 0 a 9, as letras maiúsculas e os símbolos $, %, *, +, –, / e : bem como um espaço. Embora represente a informação de forma mais compacta, não abarca letras minúsculas ou outros símbolos além dos supracitados. Por fim, o modo Kanji é para caracteres japoneses e é pouco utilizado.

Para interessados em maiores detalhes e aprofundamentos, o documento de especificação do QR code é o ISO/IEC 18004:2015, porém não poderá ser obtido por meios legais sem o desembolso de uma quantia razoável. Eby (2015) também nos apresenta gratuitamente um ótimo tutorial para interessados em se aprofundar na geração de QR codes ou entusiastas da programação. Porém, o exemplo acima, apesar de simples, já evidencia dificuldades relevantes ao se trabalhar profissionalmente com essa tecnologia. Na próxima seção veremos como contornar esse obstáculo.

4.4 Leitura e Geração de QR Codes

Evidentemente, como pode-se perceber pela própria história da invenção dos códigos de barras, nem eles e muito menos os QR codes foram feitos para o "olho humano". Muito pelo contrário, o objetivo sempre foi facilitar e tornar mais rápidos os processos envolvidos no uso dessas tecnologias. Felizmente, atualmente é relativamente simples encontrar meios de utilização dessas tecnologias sem a necessidade de conhecimentos técnicos significativos.

Um dos principais motivos para o avanço desse tipo de tecnologia, certamente é a praticidade gerada por aparelhos cada vez mais potentes. A melhoria das câmeras e o acesso à internet diretamente pelos smartphones permite que as pessoas apontem para um código QR em uma embalagem de produto, revista, etc. e sejam direcionadas para páginas de internet que podem conter imagens, vídeos, ou mais informações sobre determinado artigo.

Caso não haja um leitor de QR code nativo do próprio smartphone, interessados em fazer a leitura desses códigos de forma rápida e prática, podem fazer download de

um dos diversos aplicativos apropriados disponíveis na internet. O aplicativo e até as funcionalidades podem variar de acordo com o sistema operacional do aparelho.

Muitos desses aplicativos são gratuitos e funcionarão perfeitamente para a maioria dos prováveis interessados. Outros, em virtude de oferecerem mais funcionalidades como funções de estatísticas, por exemplo, são pagos. Também há leitores de QR code disponíveis para serem usados no próprio computador sem a necessidade de um smartphone. Para encontrá-los basta uma rápida pesquisa em um site de buscas.

Para adquirir um desses aplicativos para o aparelho telefônico, basta entrar na loja do respectivo sistema operacional e pesquisar por "qr code". Para um usuário de Android, por exemplo, entra-se no Google Play e pesquisa-se por "qr code" ou alguma variação desse nome. Para um usuário de Windows Phone, basta procurar pelo ícone "Loja" e igualmente fazer uma busca por "qr code" que aparecerão diversas opções. Para outros sistemas, salvas as devidas diferenças, o processo é igualmente simples. Alguns dos resultados mais comuns podem ser:

- QR Code Reader
- Scan
- QR Barcode Scanner
- ScanLife
- I-Nigma
- Barcode Scanner

Igualmente fácil é encontrar um meio de criar seu próprio código QR. Existem aplicativos para smartphones que também são geradores de QR code. Diversos sites oferecem o serviço de criação de códigos QR. Boa parte desses geradores visa à cobrança por outros serviços que também oferecem, como monitoramento de consultas, endereço dinâmico e produtos personalizados. Aqui está uma pequena lista de alguns sites em que se pode gerar QR codes de maneira gratuita:

- http://mqr.kr
- http://br.qr-code-generator.com
- http://goqr.me
- http://qrcode.kaywa.com
- http://app.qreateandtrack.com

- http://www.qrstuff.com

Para facilitar a compreensão, daremos dois exemplos de como criar seu próprio QR code. Para tais exemplos, utilizaremos o site http://mqr.kr da empresa Creative Must.

Alguns sites podem oferecer, gratuitamente, mais opções de personalização que outros, bem como alguns podem incluir novos serviços ou mesmo desaparecerem com o tempo. O site usado nos exemplos a seguir, permite modificações tais como coloração e versão do código QR. Antes de modificar as cores, é importante lembrar que deve haver contraste suficiente entre as cores usadas no fundo do código e os demais campos.

Siga os passos abaixo para criar um QR Code que contém apenas um texto (figura 4.7):

1. Acesse o site http://mqr.kr;
2. Clique no ícone “Free Formatted Text”;
3. 3. No campo apropriado, digite “QR Code de TEXTO”;
4. Escolha um dois seis formatos predefinidos em “Quick Settings”;
5. Se desejar, clique em “Show advanced settings” e faça modificações;
6. Clique no botão para gerar o código, “Generate”;
7. Clique no código gerado com o botão direito do mouse e escolha “Salvar imagem como” para salvá-la onde preferir.

Figura 4.7 – QR Code de Texto.

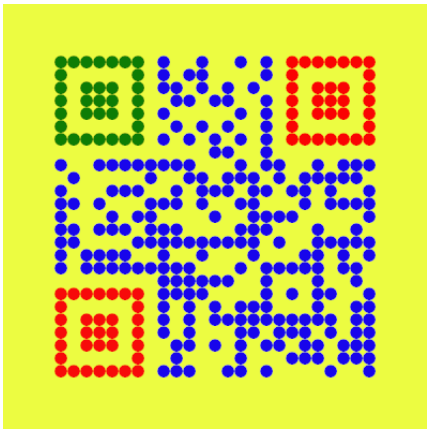
Fonte: Código gerado pelo site http://mqr.kr.

Um QR Code pode ter várias outras funcionalidades: fazer uma chamada telefônica, guardar dados de um contato em seu aparelho, enviar um e-mail, etc. Uma das funções

mais frequentes é levar o usuário a uma determinada página de internet. Então, seguindo novamente os passos, será gerado um QR code com um link para uma página de internet (figura 4.8):

1. Acesse o site "http://mqr.kr";
2. Clique no ícone "Browse to a Website";
3. Digite o endereço desejado no campo correspondente (ex.: http://www.google.com);
4. Escolha um dos formatos de código QR que aparecem em "Quick Settings";
5. Se desejar, clique em "Show advanced settings" e faça modificações;
6. Clique no botão para gerar o código, "Generate";
7. Clique no código gerado com o botão direito do mouse e escolha "Salvar imagem como" para salvá-lo em seu computador onde preferir.

Figura 4.8 – QR Code para Página de Internet.



Fonte: Código gerado pelo site http://mqr.kr.

4.5 Outros Códigos Bidimensionais

Apesar de ser um dos mais famosos, o código QR não foi o primeiro e não é o único código de barras bidimensional. Entre alguns dos mais famosos está o Datamatrix (figura 4.9), projetado em 1989 e que se caracteriza pela borda sólida em L e pelas duas bordas opostas serrilhadas. Assim como o QR, necessita de uma borda branca ao redor para garantir uma boa leitura sem interferência de imagens circundantes.

O Shotcode (figura 4.10) é um código de barras circular criado pelo Laboratório de Computação da Universidade de Cambridge em 1999. Pode ser lido por aplicativos de

Figura 4.9 – Datamatrix.

Fonte: https://en.wikipedia.org/wiki/Data_Matrix.

smartphones e é usado em grande parte das vezes para direcionar usuários para páginas de internet.

Figura 4.10 – Shotcode.

Fonte: https://en.wikipedia.org/wiki/ShotCode.

O Beetagg foi desenvolvido na Alemanha e já previa espaços para logos em seu interior. Acabou perdendo espaço pela possibilidade de estilização também dos QR codes. Na figura 4.11 é possível perceber a presença de hexágonos no lugar dos tradicionais quadradinhos ou barras.

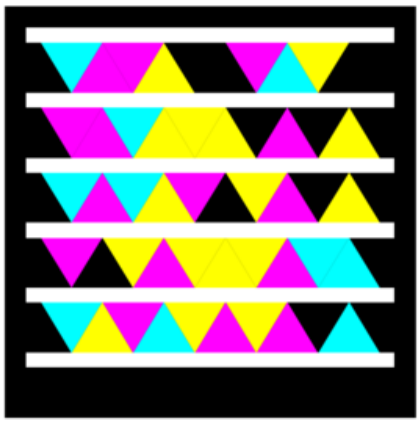
Também diferenciando um pouco dos pixels quadrados, a Microsoft criou seu próprio código que utiliza conjuntos de triângulos coloridos. A densidade dos dados é aumentada pela utilização de uma gama de quatro ou oito cores para os triângulos. É possível utilizar somente preto e branco também. Na figura 4.12 temos um exemplo do Microsoft Tag.

O Aztec Code tem como característica um quadrado localizado no centro do código.

Figura 4.11 – Beetag.

Fonte: http://www.beetagg.com/en/what-is-beetagg/.

Figura 4.12 – Microsof Tag.



Fonte: https://pl.wikipedia.org/wiki/Microsoft_Tag.

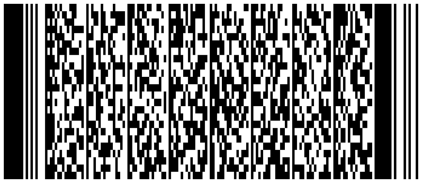
É um padrão comum para cartões de embarque visualizados por smartphones como exemplificado pela figura 4.13.

A figura 4.14 ilustra o PDF-417 (Portable Data File-417), que foi originalmente publicado pela empresa americana Symbol Technologies para preencher a necessidade de códigos de barras de maior densidade. São usados, por exemplo, pela FedEx para controle de suas cargas.

Figura 4.13 – Cartão de Embarque Recebido no Celular.

Fonte: http://www.mobiliodevelopment.com/aztec-code-2d-barcode/.

Figura 4.14 – PDF-417.



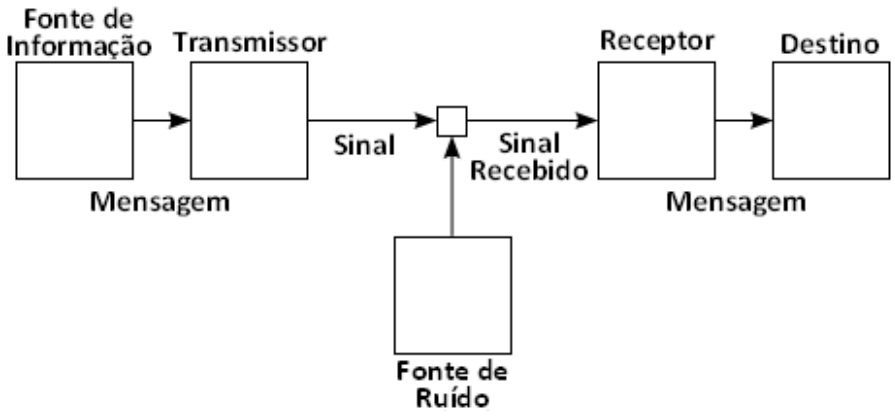
Fonte: https://en.wikipedia.org/wiki/PDF417.

5 UM POUCO SOBRE ERROS

Não é difícil imaginar que na transmissão de uma informação ou, mais precisamente, um código podem ocorrer erros. Estes podem surgir na própria codificação dos dados originais, no canal de transmissão ou mesmo na leitura (decodificação) do mesmo. Como, obviamente a informação, o código, não pode simplesmente ser descartado ou utilizado de forma inadequada, faz-se necessário o estudo de métodos que permitam detectar e corrigir erros.

A teoria dos códigos corretores de erro é uma subárea da teoria da informação e lida com o problema da transmissão de mensagens de forma confiável. O trabalho *"A Mathematical Theory of Communication"* de Claude Elwood Shannon (SHANNON, 1948), publicado em 1948, é tido como o marco inicial da teoria da informação. Nesse trabalho Shannon já indica a ocorrência de interferências no processo de transmissão de dados entre emissor e receptor esquematizado na figura 5.1.

Figura 5.1 – Diagrama de um Sistema de Comunicação em Geral.



Fonte: https://en.wikipedia.org/wiki/A_Mathematical_Theory_of_Communication[1].

O objetivo deste capítulo, contudo, não é um aprofundamento na teoria dos códigos corretores de erro, pois exigiria conhecimentos de álgebra e cálculo que fogem ao escopo deste trabalho. Para o leitor interessado em se aprofundar um pouco mais, sugerimos as referências Lavor et al. (2006), Milies (2009a) e Ventura (2013). Entretanto, abordaremos de forma simplificada alguns aspectos gerais e exemplos práticos.

[1] Traduzido pelo autor.

5.1 Conceitos Básicos

Conforme sugerido por Milies (2009a), os idiomas são o mais comum dos códigos utilizados para os seres humanos e inspiram a construção de outros. Na Língua Portuguesa usamos um alfabeto de 26 letras e, com sequências (finitas) dessas letras, formamos as palavras. Evidentemente nem todas as sequências de letras que podem ser formadas compõe a nossa língua. Reconhecemos algumas delas como parte da língua e outras não.

Através desse exemplo do idioma podemos, de forma simplificada, destacar os elementos básicos para a construção de um código:

- Alfabeto - composto por um número finito de elementos que são as letras no nosso exemplo;
- Palavras - que são sequências finitas de símbolos do alfabeto;
- Comprimento - o número de letras das palavras. Se todas as palavras do código têm o mesmo comprimento, então ele é dito uniforme;
- Código q-ário - é um subconjunto não vazio de palavras do alfabeto de $q \geq 1$ elementos. Se $q = 2$, por exemplo, o código diz-se binário.

Como já foi dito, no processo de transmissão de dados podem ocorrer interferências. Alguém poderá sugerir que se envie novamente a mensagem quantas vezes forem necessárias, porém isso nem sempre será possível. A confiabilidade pode ser aumentada inserindo-se algum tipo de redundância como a repetição de cada palavra, por exemplo.

Quando a mensagem, a informação, é pequena, podemos simplesmente repeti-la várias vezes na transmissão. Uma mensagem como "Bom Trabalho" poderia ser enviada *"Bom Trabalho Bom Trabalho Bom Trabalho"* e assim verifica-se a existência de erros comparando-as todas. Se a mensagem recebida for *"Bom Trabalho Bom Tlabalho Bom Trabalho"*, percebemos que há discordância nas mensagens e identificamos o erro. Outro exemplo simples é a adoção de um bit de redundância (bit de paridade). As mensagens *"00, 01 e 11"* podem ser enviadas como *"000, 011 e 110"* onde o terceiro bit é 0 se houver quantidade par de bits iguais a 1 na mensagem original, e 1 se a quantidade for ímpar. Desse modo, a contagem final será sempre par. Mas a redundância tem sempre custo, e um dos desafios da teoria dos códigos é adquirir confiabilidade ao menor custo possível.

Escolher um código melhor que outro dependerá do sentido que se der à palavra "melhor". Levar-se-á em conta certas características como velocidade de transmissão, facilidade e eficiência de codificar e decodificar, capacidades de detecção e correção de erros, etc. Um código de comprimento menor será mais rápido de se transmitir enquanto que um código com a informação triplicada, por exemplo, permitirá detectar erros e até corrigi-los, porém não será "econômico".

Suponha que recebamos uma mensagem com a palavra *teorxa*. É evidente que a mensagem contém um erro porque tal palavra não pertence a nossa língua. Observe também que acreditamos que a mensagem correta seja *teoria*, pois é a palavra mais "próxima" da mensagem recebida. Por outro lado, se a mensagem recebida fosse *wato*, haveria opções de correção igualmente "próximas" como *mato, pato, gato, tato, etc.*

Esse exemplo remete claramente aos corretores ortográficos que ao verificarem que uma palavra não consta em seu dicionário interno, acusam um erro. Se houver uma palavra suficientemente "próxima", eles podem até "corrigi-la" automaticamente.

Essa noção de "proximidade" é geralmente expressa por uma função distância. Uma função distância muito utilizada é a distância de Hamming que conta o número de símbolos diferentes entre duas palavras-código (de mesmo tamanho): dados dois pontos $x = (x_1, x_2, ..., x_n)$ e $y = (y_1, y_2, ..., y_n)$ de um espaço A^n, definimos a **distância de Hamming** entre x e y como

$$d(x, y) = |\{i | x_i \neq y_i, 1 \leq i \leq n\}|.$$

A distância de Hamming definida acima é, de fato, uma distância no sentido matemático do termo, pois satisfaz as seguintes propriedades:

i) $d(x, y) \geq 0$ para todos $x, y \in A^n$;

ii) $d(x, y) = 0 \Leftrightarrow x = y$;

iii) $d(x, y) = d(y, x)$ para todos $x, y \in A^n$;

iv) $d(x, z) \leq d(x, y) + d(y, z)$ para todos $x, y, z \in A^n$ (desigualdade triangular).

Em palavras com o mesmo comprimento, por exemplo, a distância entre elas seria a quantidade de letras em que divergem. Assim a mensagem *matxmática* estaria à distância de 1 (um) de *matemática* e 2 (dois) de *matemático* e consequentemente poderia ser "corrigida" com substituição pela primeira. Já a mensagem *wato* estaria a uma mesma distância das palavras *nato, fato, bato, etc.*

Desse modo, ao receber um elemento, podemos perceber se ele contem erro desde que tenhamos um critério claro para decidir se ele pertence, ou não, ao código. Por outro lado, para substituir o elemento recebido com erro pelo mais próximo, é necessário que não haja ambiguidade na determinação de tal elemento.

Quanto mais palavras um código possuir mais eficiente ele será, pois poderá transmitir mais mensagens, informação. Por sua vez, o comprimento das palavras influi na taxa de transmissão e uma distância mínima relativamente grande entre as palavras permite uma melhor capacidade de correção de erros. Porém, o fato de aumentar a quantidade de

palavras implica justamente em diminuir a distância entre elas. A questão de encontrar valores satisfatórios para o maior número de palavras que um código pode conter, seu comprimento e a distância mínima entre elas, é conhecida como o problema principal da teoria de códigos.

5.2 Aplicações de Detectores de Erros

Já sabemos que os códigos estão presentes em nossa vida diária e mesmo assim a maioria deles passa completamente despercebida no nosso cotidiano. Entretanto há pessoas cujo ofício exige o manuseio e digitação de enormes quantidades desses códigos, como um caixa de banco ou supermercado, por exemplo. Infelizmente, muitas vezes são cometidos erros de digitação.

Pensando nisso, seria bom que houvesse uma forma de identificar alguns desses erros de digitação. E esse é justamente o papel dos dígitos de controle que apesar de não poderem detectar todos os erros que podem ocorrer durante uma digitação, são capazes, segundo Mello (2002), de identificar 90% dos erros mais frequentes que são a digitação equivocada de um número (79%) e a troca de dois dígitos contíguos (11%). Ainda segundo Mello (2002), os demais 10% estão distribuídos em diversas categorias em que nenhuma delas representa mais que 1% do total. Nessa seção veremos algumas aplicações desses códigos detectores de erro.

5.2.1 EAN-13 e UPC

No capítulo 3, vimos que os doze primeiros dígitos de um código de barras no padrão EAN-13 já estão definidos pela identificação do país de origem, fabricante e produto. Agora veremos como obter o décimo terceiro algarismo que é utilizado para detecção de erros. Para isso, vamos utilizar noções de vetor e produto escalar. O leitor interessado em mais detalhes sobre o assunto pode consultar Lipschutz e Lipson (2011, p. 10-11)

Dados dois vetores $u = (u_1, u_2, ..., u_n)$ e $v = (v_1, v_2, ..., v_n)$ de $\mathbb{R}^n$, o **produto escalar** de u e v é denotado e definido por

$$u \cdot v = u_1v_1 + u_2v_2 + ... + u_nv_n$$

ou seja, $u \cdot v$ é obtido com a multiplicação dos componentes correspondentes e com a soma dos produtos resultantes. Como exemplo, sejam os vetores $u = (3, -1, 2)$ e $v = (7, 5, 3)$. Então

$$u \cdot v = 3.7 + (-1).5 + 2.3 = 21 - 5 + 6 = 22.$$

Agora, voltando ao código de barras, suponha que a sequência de dígitos $n_1n_2n_3...n_{13}$ seja um produto identificado no sistema EAN-13. Denotaremos o décimo terceiro dígito

por x e, para simplificar a exposição, vamos escrever a sequencia em forma de um vetor $n = (n_1, n_2, n_3, ..., x)$.

No sistema EAN-13 utilizamos um vetor $p = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$ que chamaremos de vetor pesos. Agora calculamos o produto escalar entre os vetores n e p. Ou seja, multiplicamos cada dígito do vetor n pelo número que ocupa a mesma posição no vetor pesos, p, e somamos:

$$n \cdot p = (n_1, n_2, n_3, ..., x) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$$

$$n \cdot p = n_1 + 3n_2 + n_3 + 3n_4 + n_5 + 3n_6 + n_7 + 3n_8 + n_9 + 3n_{10} + n_{11} + 3n_{12} + x$$

Então, o dígito verificador x é escolhido de modo que a soma obtida seja múltiplo de 10.

Para exemplificar, tomemos o código apresentado na figura 5.2 (7899563210352) e cujo algorítimo do dígito verificador é descrito pela tabela 5.1:

Figura 5.2 – Dígito Verificador em EAN-13.

Fonte: feito pelo autor.

Tabela 5.1 – Calculando Dígito Verificador - EAN-13.

Código de Barras	**9**	**7**	**8**	**8**	**5**	**6**	**1**	**8**	**9**	**3**	**0**	**0**	**X**
Vetor Pesos	1	3	1	3	1	3	1	3	1	3	1	3	1
Produto	9	21	8	24	5	18	1	24	9	9	0	0	X
Soma	128 + X												

Fonte: feito pelo autor.

Como o próximo número divisível por 10 depois de 128 é 130, o dígito de controle só pode ser $130 - 128 = 2$.

Assim, se um digitador cometer um erro "detectável" (alguns erros podem se compensar), o computador faz a leitura e ao realizar a operação obtém um número que não é múltiplo de 10. Nesse caso, emite um sinal avisando que algum erro foi cometido.

Para um código no padrão UPC, o processo é muito semelhante. Como um código UPC tem apenas 12 dígitos, basta usar o vetor pesos $p = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$ que também tem um dígito a menos, ou acrescentar um zero no início do código de barras UPC que é justamente o que acontece com a ideia de compatibilidade entre os padrões UPC e EAN vista no capítulo 3.

Figura 5.3 – Dígito Verificador UPC-A.

Fonte: feito pelo autor.

Logo, para o código da figura 5.3, o produto escalar entre o vetor código, $n = (0, 4, 7, 8, 7, 5, 8, 7, 3, 2, 3, x)$, e o vetor pesos, $p = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$, é igual a $110 + x$. Como 110 já é um múltiplo de 10, $x = 0$ (que confere com o exemplo). A tabela 5.2 descreve o processo de cálculo do dígito verificador para um código UPC-A.

Tabela 5.2 – Calculando Dígito Verificador - UPC-A.

Código UPC-A	**0**	**4**	**7**	**8**	**7**	**5**	**8**	**7**	**3**	**2**	**3**	**X**
Vetor Pesos	3	1	3	1	3	1	3	1	3	1	3	1
Produto	0	4	21	8	21	5	24	7	9	2	9	X
Soma	110 + X											

Fonte: feito pelo autor.

5.2.2 Sistema ISBN

O registro ISBN (International Standart Book Number) é um sistema internacionalmente adotado para a classificação de livros. O código é composto por "nove dígitos

significativos", como pode ser notado na figura 5.4. O "prefixo 978" foi adotado a partir de 1º de janeiro de 2007 e quando ele se esgotar, será adotado o "prefixo 979".

Figura 5.4 – Código ISBN.

Fonte: http://isbn.world.

Para um código ISBN representado pelo vetor $n = (n_1, n_2, n_3, ..., n_9, x)$, utiliza-se o vetor de pesos $p = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$ e escolhe-se o dígito de verificação de modo que o produto escalar, $n \cdot p$, seja múltiplo de 11. Assim, para o número ISBN 978-85-61893-00-1, presente em Couto (2008), teríamos:

$$(8, 5, 6, 1, 8, 9, 3, 0, 0, x) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) = 285 + x$$

Como o próximo múltiplo de 11 após 285 é 286, temos $x = 1$ que confere com a referência apresentada. Lembremos que os código ISBN puro, que é usado para o cálculo do dígito verificador, é composto apenas pelos números 85-61893-00.

Quando o dígito verificador encontrado for 10, ele será representado pela letra X (não confundir com a incógnita "X" da tabela 5.3), para que o código não ultrapasse o "limite de dígitos".

Tabela 5.3 – Calculando Dígito Verificador - ISBN.

Código ISBN	**8**	**5**	**6**	**1**	**8**	**9**	**3**	**0**	**0**	**X**
Vetor Pesos	10	9	8	7	6	5	4	3	2	1
Produto	80	45	48	7	48	45	12	0	0	X
Soma	285 + X									

Fonte: feito pelo autor.

5.2.3 CPF ou EAN-11

O CPF é um número fornecido pela Receita Federal, usado para cadastramento de pessoas físicas no Brasil. Segundo Fini (2009), ele é um EAN-11 onde os oito primeiros algarismos são o número-base, o nono indica a unidade da federação (quadro 11) onde a pessoa fez o registro e os dois últimos são algarismos de controle obtidos dos demais.

Quadro 11 – Código EAN-11 para Unidades da Federação.

CÓDIGO EAN-11 PARA AS UNIDADES DA FEDERAÇÃO	
Brasil	
0	Rio Grande do Sul
1	Distrito Federal, Goiás, Mato Grosso, Mato Grosso do Sul e Tocantins
2	Acre, Amapá, Amazonas, Pará, Rondônia e Roraima
3	Ceará, Maranhão e Piauí
4	Alagoas, Paraíba, Pernambuco e Rio Grande do Norte
5	Bahia e Sergipe
6	Minas Gerais
7	Espírito Santo e Rio de Janeiro
8	São Paulo
9	Paraná e Santa Catarina

Fonte: FINI, 2009, p.74.

Apesar da presença de dois dígitos verificadores no CPF, o método para calcular cada um deles é semelhante aos que já foram vistos até aqui:

- Primeiro multiplicamos cada um dos nove primeiros dígitos do código por 1, 2, 3, 4, 5, 6, 7, 8 e 9, respectivamente;
- Depois somamos esses produtos e dividimos por 11;
- O resto dessa divisão é o primeiro dígito de controle;
- Juntamos o dígito encontrado aos anteriores e temos um novo número composto por dez dígitos;
- Agora multiplicamos cada um desses dez dígitos respectivamente por 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9;

- Mais uma vez somamos os produtos obtidos e dividimos por 11;
- O resto dessa última divisão será o segundo dígito de controle;
- O resto 10 é considerado 0 (zero).

Para o CPF 136.985.516-83, por exemplo, teríamos:

$$(1, 3, 6, 9, 8, 5, 5, 1, 6) \cdot (1, 2, 3, 4, 5, 6, 7, 8, 9) = 228$$

Cujo resto da divisão por 11 é 8, de onde segue

$$(1, 3, 6, 9, 8, 5, 5, 1, 6, 8) \cdot (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) = 256$$

Novamente, calculando o resto da divisão por 11, obtemos 3. A tabela 5.4 apresenta cada etapa desse processo.

Tabela 5.4 – Dígitos Verificação - CPF.

Código CPF (9 prim.)	**1**	**3**	**6**	**9**	**8**	**5**	**5**	**1**	**6**	d_1	d_2
Vetor Pesos	1	2	3	4	5	6	7	8	9		
Produto	1	6	18	36	40	30	35	8	54		
Soma					228						
Resto por 11					8						$d_1 = 8$
Código CPF (10 prim.)	**1**	**3**	**6**	**9**	**8**	**5**	**5**	**1**	**6**	**8**	d_2
Vetor Pesos	0	1	2	3	4	5	6	7	8	9	
Produto	0	3	12	27	32	25	30	7	48	72	
Soma					256						
Resto por 11					3						$d_2 = 3$
CPF (completo)	**1**	**3**	**6**	**9**	**8**	**5**	**5**	**1**	**6**	**8**	**3**

Fonte: feito pelo autor.

Observe que tanto o EAN-13, o ISBN e o CPF são exemplos de códigos que detectam mas não corrigem um erro. Suponha que o código EAN-13 7894900011513 tenha sido digitado. O processo de verificação apresentado anteriormente indica que um erro foi cometido, mas onde? Como corrigir? Ainda que restrinjamos a correção aos produtos de um estoque hipotético, a figura 5.5 mostra que há duas possibilidades igualmente válidas para o código, porém não há a menor indicação de que o erro tenha sido cometido ao digitar 1 em vez de 9 no penúltimo algarismo ou 3 em lugar do 7 no último dígito.

Também é possível que alguns erros não sejam percebidos ou que o acúmulo deles termine por se compensar. Mas antes de decretar a ineficiência de um desses códigos, lembre-se que algumas ocorrências são tão pequenas que pode não "compensar" tentar contorná-las. Um código que apenas detecte 90% dos erros cometidos pode ser uma opção

Figura 5.5 – Detecção de Erro sem Correção.

Fonte: http://isbn.world.

"melhor" do que um com capacidade de detecção e correção mais elevados, mas que exija troca de maquinário e manutenções complexas e custosas.

6 SUGESTÕES DE ATIVIDADES

Neste capítulo apresentaremos algumas propostas de atividades com o objetivo de contribuir com o aprendizado teórico da matemática do ensino básico, suas aplicações e despertar interesse nos alunos por assuntos matemáticos. Embora as atividades não tenham sido testadas em sala de aula, espera-se que seja possível implementá-las e adaptá-las em momentos oportunos de acordo com o interesse do professor.

Através do capítulo 5, sobre erros, é possível perceber que os códigos são um campo rico para exploração da aritmética no ensino fundamental e mesmo da álgebra no ensino médio. Por meio de tais códigos podemos estimular e aprimorar a leitura e interpretação de tabelas, fórmulas e dos próprios códigos. Ainda podemos reforçar e destacar propriedades básicas de operações como soma, multiplicação e divisão, potenciação, cálculos mentais e linguagem algébrica para escrever algoritmos.

Esperamos que as sugestões aqui apresentadas sirvam de ponto de partida para outras atividades ou mesmo aperfeiçoamento das mesmas, visto que tanto nas referências usadas (ECKSCHMIDT; MORITA, 2014; TOLEDO, 2012; SANSWEET, 2011) quanto na internet encontram-se diversas sugestões para uso criativo da tecnologia como, por exemplo, o envio do boletim do aluno aos pais com QR codes que permitam acessar as notas online com a descrição das atividades realizadas e o desempenho do aluno em cada uma delas.

6.1 Criando Seu Código Bidimensional

O objetivo dessa atividade é explorar a necessidade de coletividade inerente ao ser humano e o interesse despertado pela escrita em códigos para criar um tipo de "QR code simplificado" que possa identificar os alunos de determinada turma em uma escola.

Para o nosso código, vamos usar a tabela ASCII que é de uso comum para representação de textos em computadores e outros dispositivos, além de já termos tido uma pequena familiarização com ela na leitura de um QR code no capítulo 4.

Uma letra, um número ou símbolo representado nessa tabela usa uma sequencia de 8 bits (0's e 1's) formando um byte. Nela podemos representar os números de 0 a 9, letras maiúsculas e minúsculas, além de outros sinais. Como podemos expressar 256 combinações diferentes com 8 bits, cada byte da tabela ASCII possui um bit excedente que pode ser utilizado de formas diferentes como verificação de paridade para checagem de erros, similarmente ao visto no capítulo anterior. A tabela 6.1 apresenta sinais gráficos imprimíveis do padrão ASCII.

Tabela 6.1 – Caracteres Imprimíveis da Tabela ASCII.

Bin	**Dec**	**Sinal**	**Bin**	**Dec**	**Sinal**	**Bin**	**Dec**	**Sinal**
0010 0000	32	(espaço)	0100 0000	64	@	0110 0000	96	`
0010 0001	33	!	0100 0001	65	A	0110 0001	97	a
0010 0010	34	”	0100 0010	66	B	0110 0010	98	b
0010 0011	35	#	0100 0011	67	C	0110 0011	99	c
0010 0100	36	$	0100 0100	68	D	0110 0100	100	d
0010 0101	37	%	0100 0101	69	E	0110 0101	101	e
0010 0110	38	&	0100 0110	70	F	0110 0110	102	f
0010 0111	39	’	0100 0111	71	G	0110 0111	103	g
0010 1000	40	(	0100 1000	72	H	0110 1000	104	h
0010 1001	41	)	0100 1001	73	I	0110 1001	105	i
0010 1010	42	*	0100 1010	74	J	0110 1010	106	j
0010 1011	43	+	0100 1011	75	K	0110 1011	107	k
0010 1100	44	,	0100 1100	76	L	0110 1100	108	l
0010 1101	45	-	0100 1101	77	M	0110 1101	109	m
0010 1110	46	.	0100 1110	78	N	0110 1110	110	n
0010 1111	47	/	0100 1111	79	O	0110 1111	111	o
0011 0000	48	0	0101 0000	80	P	0111 0000	112	p
0011 0001	49	1	0101 0001	81	Q	0111 0001	113	q
0011 0010	50	2	0101 0010	82	R	0111 0010	114	r
0011 0011	51	3	0101 0011	83	S	0111 0011	115	s
0011 0100	52	4	0101 0100	84	T	0111 0100	116	t
0011 0101	53	5	0101 0101	85	U	0111 0101	117	u
0011 0110	54	6	0101 0110	86	V	0111 0110	118	v
0011 0111	55	7	0101 0111	87	W	0111 0111	119	w
0011 1000	56	8	0101 1000	88	X	0111 1000	120	x
0011 1001	57	9	0101 1001	89	Y	0111 1001	121	y
0011 1010	58	:	0101 1010	90	Z	0111 1010	122	z
0011 1011	59	;	0101 1011	91	[	0111 1011	123	{
0011 1100	60	<	0101 1100	92	\	0111 1100	124	|
0011 1101	61	=	0101 1101	93	]	0111 1101	125	}
0011 1110	62	>	0101 1110	94	ˆ	0111 1110	126	∼
0011 1111	63	?	0101 1111	95	_			

Fonte: https://pt.wikipedia.org/wiki/ASCII.

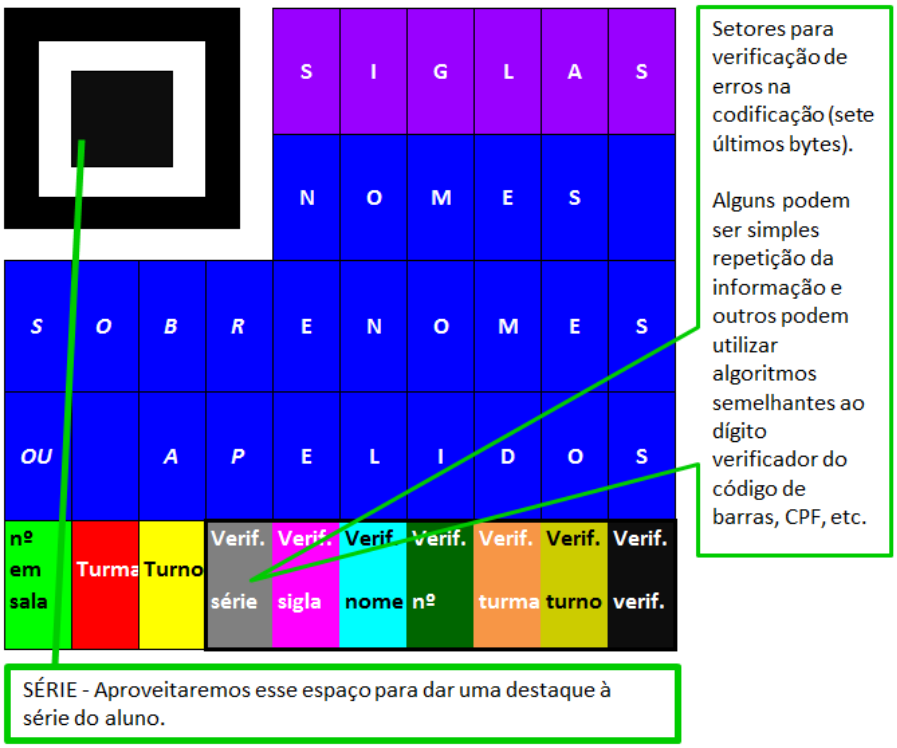
Claro que o professor pode criar seu próprio código com os alunos da maneira que achar mais conveniente. Mas aqui, utilizaremos essa tabela de forma a trabalhar com um conteúdo já padronizado e expandir os horizontes para uma linguagem aparentemente comum no mundo tecnológico. Além de estimular a leitura, compreensão e tratamento de informações presentes em tabelas.

O primeiro passo é definir quais informações devem ser apresentadas no código e o tamanho necessário:

- Sigla da instituição de ensino - algo em torno de 6 bytes;
- Nome do aluno - 26 bytes devem ser mais do que o suficiente para expressar qualquer nome composto, sobrenomes e até apelidos;
- Número - 1 byte;
- Série - 1 byte;
- Turma - 1 byte;
- Turno - 1 byte;

No nosso exemplo, criamos um símbolo grande o suficiente para que se possa escrever os nomes sem problemas, e ainda temos espaço para aplicar campos verificadores de erro e nos aproveitar deles para elaborar questões que permitam explorar a aritmética e álgebra.

Figura 6.1 – Código Personalizado.



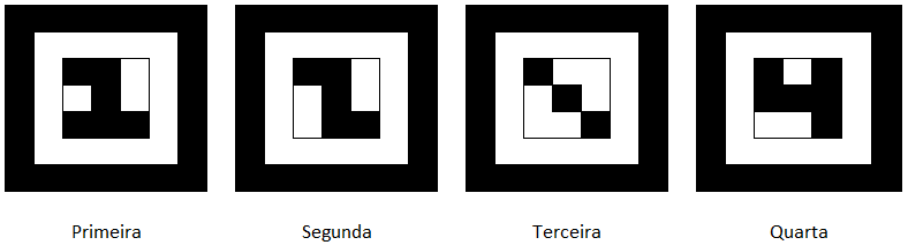
Fonte: feito pelo autor.

Percebemos pela figura 6.1, que, diferentemente da leitura do QR code apresentada no capítulo 4, nosso código é lido da esquerda para a direita em cada "linha" como se estivéssemos lendo um texto normal. Se algum elemento, como uma figura, for inserido no código é importante que a forma de leitura esteja bem definida. Aqui, convencionaremos

que a leitura só deve passar para a linha de baixo depois de atingir o fim da linha atual. Ou seja, "saltamos" o obstáculo e continuamos a leitura na mesma linha.

Também vamos aproveitar o quadrado do canto superior esquerdo para expressar a série do aluno. O código que representará cada série pode ser estabelecido previamente entre o professor e seus alunos e aproveitar-se criativamente da grande variedade de sinais representáveis. Na figura 6.2, percebemos que é possível até mesmo representar alguns números na forma convencional.

Figura 6.2 – Representação de Séries.



Fonte: feito pelo autor.

Para exemplificar, tomemos o caso hipotético de um aluno que estude no turno matutino de um colégio cuja sigla é CESRS e só tem turmas de ensino médio regular (1ª, 2ª e 3ª séries). Sua série é a 3ª (terceiro ano), seu nome Deivison Porto de Sousa, seu número na lista de chamada 7 (sete) e sua turma a G (3º G).

Agora usamos a tabela ASCII para codificar as informações em nosso símbolo. Antes é preciso definir parâmetros para prevenir certas ambiguidades. O turno, por exemplo, pode ser diferenciado pelos números 1, 2 e 3 respectivamente para matutino, vespertino e noturno ou pelas iniciais M, V e N. No nosso exemplo, usaremos as iniciais. Espaços vazios no final da sigla ou nome podem ser deixados assim mesmo, preenchidos com o byte de espaço (00100000) ou com alguma outra sequência não utilizada e que seja mais conveniente como talvez 00000001. Usaremos esta última que quando convertida para decimal equivale ao número 1.

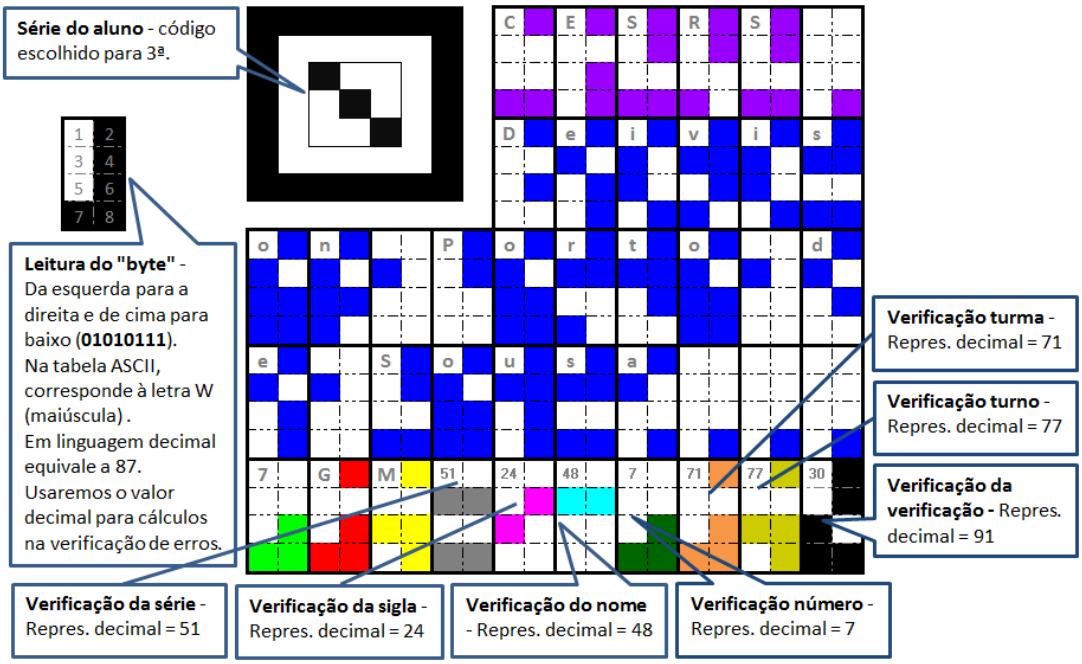
Por fim, o número do aluno merece atenção especial. Na tabela ASCII temos apenas os algarismos de 0 a 9, mas o número do aluno pode ser igual ou maior que 10. Então, nesse campo, o número será representado pelo seu verdadeiro valor na base 2 e não através da tabela ASCII. Para o $(7)_{10}$ temos $(00000111)_2$.

Finalmente, vamos a nossa representação:

- 3ª série - vide figura 6.2;
- Sigla da escola - CESRS;
- Nome do aluno - Deivison Porto de Sousa;

- Número na caderneta - 7 (00000111);
- Turma - G;
- Turno - M.

Figura 6.3 – Código do Aluno Pronto.



Fonte: feito pelo autor.

A figura 6.3 exemplifica o código de aluno pronto e esclarece aspectos gerais sobre leitura dos bytes. Os últimos sete bytes, no entanto merecem uma explicação minuciosa, apesar dos seus aspectos fundamentais poderem ser alterados:

- Verificação da série - apenas "escrevemos" o número que representa a série do aluno de acordo com a tabela ASCII (3 = 00110011). A representação decimal de 00110011 é 51, e é este valor que usaremos para efetuar cálculos;
- Verificação da sigla - a primeira das seis letras da sigla é C (01000011) que equivale à 67 em notação decimal. Juntamente com as outras letras formamos o vetor sigla $(67, 69, 83, 82, 83, 1)$. Semelhantemente ao que foi visto no capítulo anterior, estabelecemos o vetor pesos $(1, 2, 3, 4, 5, 6)$ e calculamos o produto escalar entre os dois. O nosso "dígito" verificador será o resto da divisão desse produto por 131. No nosso exemplo obtivemos 24 cuja notação binária é 00011000;
- Verificação do nome - para a verificação do nome, usaremos um processo bastante semelhante ao dígito verificador do código EAN-13 visto no capítulo anterior. Substituindo os valores decimais das 26 letras do estudante, o vetor nome do nosso exemplo

equivale a $(68, 101, 105, 118, 105, ..., 115, 97, 1, 1, 1)$. Realizando o produto escalar com o vetor pesos (1,3,1,3,1,3,...1,3), obtemos 4406. Nosso número de controle X será tal que $4406 + X$ seja divisível por 131. Logo, no nosso exemplo, $X = 48$ (00110000);

- Verificação do número - para verificá-lo, aproveitamos o fato de ser uma informação pequena e simplesmente a repetimos conforme os comentários sobre redundância da página 36. Lembramos que esse valor não foi dado pela tabela ASCII, mas sim pela sua representação exata na base 2. Como nosso aluno tinha o número 7, aqui ele será mais uma vez representado por sua correspondência binária 00000111 que equivale justamente a 7 em notação decimal;

- Verificação da turma - para verificação da turma, também fizemos uma repetição simples e obtivemos 01000111 (G) que equivale a 71 em notação decimal;

- Verificação do turno - analogamente, o turno (M) é 01001101 que equivale a 77;

- Verificação da verificação - finalmente, fazemos uma verificação dos números de controle para saber se eles também foram codificados corretamente definindo o vetor verificação pelos seis números anteriores. Assim, o produto escalar do vetor verificação (51,24,48,7,71,77) pelo vetor pesos (1,2,3,4,5,6) é 1088. Nosso número verificador final será X tal que $1088 + X$ seja divisível por 131. Logo, $X = 91$ (00011110).

6.1.1 Recursos

Nos parece bastante pertinente a realização dessa atividade com o auxílio de planilhas eletrônicas. Para isso seria conveniente que a escola contasse com um bom laboratório de informática com os softwares adequados instalados (Excel, Calc, etc.). Não havendo essa possibilidade o professor pode propô-la como atividade de casa ou mesmo trabalhar com impressões ou papel quadriculado e lápis de cor. Calculadoras também serão muito úteis.

6.1.2 Desenvolvimentos

O trabalho pode ser iniciado com uma pesquisa sobre códigos ou mais especificamente sobre códigos de barras. O professor pode aproveitar para apontar a linearidade dos códigos de barras de forma a induzir o aluno para que perceba a possibilidade de expansão da capacidade destes com a sobreposição de mais códigos chegando-se assim à ideia de código bidimensional.

Os exercícios a serem tirados dependerão do interesse de trabalho docente. A leitura de tabelas foi visivelmente utilizada na confecção do código que, por si só, pode constituir uma atividade fim. O trabalho com base binária pode ser enriquecido com a elaboração de

tabelas próprias ou a exclusão da coluna correspondente à parte binária da tabela ASCII, por exemplo, de forma que o aluno precise fazer a conversão por conta própria.

O estabelecimento de símbolos para a série por exemplo, permite indagar quantas representações podemos ter em um retângulo 3x3 usando apenas duas cores. As questões podem ser ampliadas com utilização de mais cores ou estabelecimento de quantidades mínimas de quadrados de determinada coloração, etc.

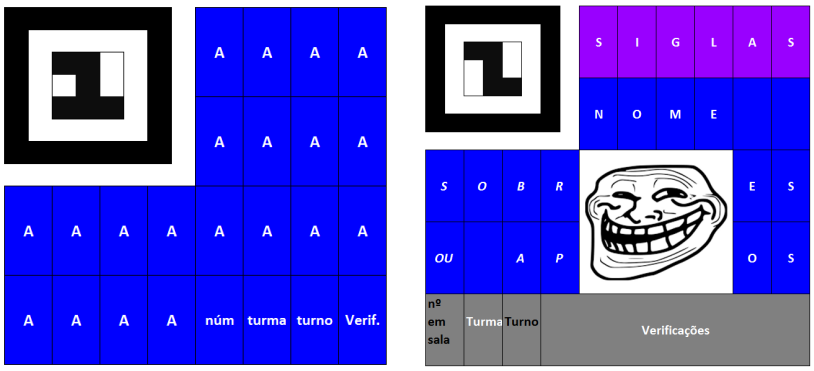
A realização da atividade com o auxilio de planilhas permite a criação de rotinas automatizadas para checagem dos números de controle e conversão de bases, além de estimular o raciocínio lógico e a linguagem algébrica através da programação. O trabalho de calcular certos resultados pode ser facilitado explorando-se determinadas propriedades de congruências ou aritmética dos restos.

6.1.3 Modificações

O exemplo dado na construção do código do aluno pode ser muito grande para construção manual, portanto, como já mencionado, o professor pode fazer adaptações para torná-lo menor e de confecção mais rápida. Pode-se omitir o "nome da escola", reduzir substancialmente o espaço para o nome do aluno de forma a simplificar a verificação de erros ou mesmo aproveitar o grande espaço para colocar imagens internas no símbolo ou até fotos (figuras 6.4(a) e 6.4(b)).

Nas verificações de sigla, nome e verificação (final), a divisão por 131 foi escolhida pelo fato dele ser um número primo (dão melhores garantias na detecção de erros) e grande o suficiente para não deixar as contas tão evidentes, porém nem tão grande para não correr o risco de ultrapassar a capacidade de representação numérica de uma sequência de oito bits (256 símbolos diferentes). Pode ser alterado tanto para facilitar os cálculos como para criação de novos exercícios sem grandes mudanças.

Figura 6.4 – Adaptações.



(a) Código reduzido (b) Com figura

Fonte: feito pelo autor.

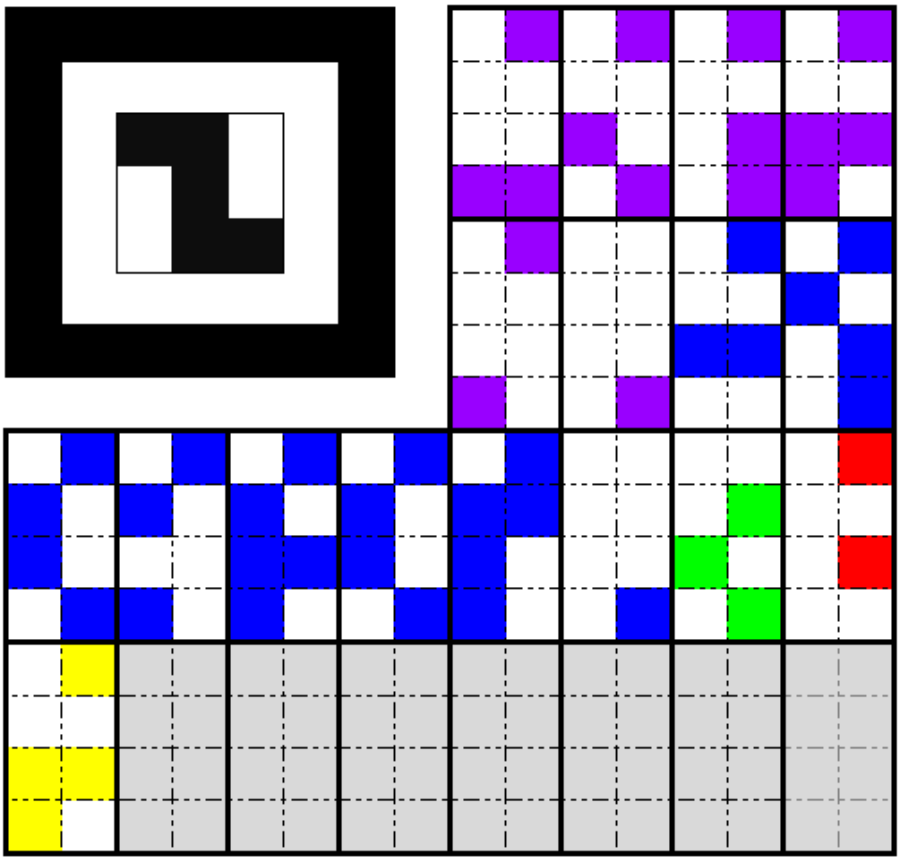
No próximo tópico, oferecemos um exemplo bem próximo de uma atividade em sala de aula. Apesar de adotarmos uma variação menor do código, ela tem todos os campos e segue os mesmos procedimentos descritos acima. A única diferença é que o campo destinado ao nome do aluno foi reduzido de 26 para 8 bytes.

6.1.4 Exemplificando

Na sala de João, o professor dividiu a turma em grupos e determinou que cada equipe fizesse um código como se algum matemático famoso fosse integrante da turma. João não ajudou os colegas e, como punição, ficou encarregado de terminar o trabalho. Porém, ele ainda perdeu as informações sobre o código e agora deve completar a atividade apenas com os dados que já foram colocados.

Com base na imagem (figura 6.5), ajude João a descobrir o nome do matemático e a preencher as informações faltantes supondo que todos os dados estejam corretos.

Figura 6.5 – Ajude João.



Fonte: feito pelo autor.

Perguntas:

1. Qual matemático foi homenageado no Código da equipe de João?

2. Qual a série desse "ilustre aluno"?

3. Qual a sigla do colégio?

4. É possível identificar qual o número do aluno, turma e turno? Em caso afirmativo, determine-os.

5. Percebe-se que a parte de verificação de erros está em branco. Com os dados apresentados é possível completar a atividade? Em caso afirmativo, apresente uma versão final para o trabalho de João.

Soluções:

1. Para a primeira pergunta devemos identificar o campo correspondente ao nome do aluno no código. Trata-se do campo em azul escuro que começa no sétimo byte. Fazendo a leitura deste e transpondo para a linguagem binária obtemos **01001100** que de acordo com a tabela ASCII representa a letra **L**. Fazendo a leitura de todos os bytes significativos do campo nome obtemos a correspondência $(01001100, 01100101, 01101001, 01100010, 01101110, 01101001, 01111010, 00000001) = (76, 101, 105, 98, 110, 105, 122, 1) = (L, e, i, b, n, i, z, 1)$.

   Lembre-se que o byte 00000001 foi definido como espaço vazio no final do texto (página 48) e, portanto, o ignoramos na leitura. Logo, nosso matemático homenageado é Gottfried Wilhelm **Leibniz** (1646-1716).

2. A série é facilmente identificável, pois está destacada no canto superior esquerdo. Segundo a convenção apresentada na figura 6.2, Leibniz está na 2ª série.

3. A sigla do colégio está alocada nos primeiros seis bytes (em roxo na figura 6.5). Novamente, fazendo a correspondência pela tabela ASCII percebemos que a sigla em em questão é CIENB: $(01000011, 01001001, 01000101, 01001110, 01000010, 00000001) = (67, 73, 69, 78, 66, 1) = (C, I, E, N, B)$.

4. O número do aluno está no 15° byte destacado pela cor verde claro. Nesse caso temos $(00011001)_2 = (25)_{10}$. Mas lembre-se que o número do aluno não está sendo convertido pela tabela ASCII e sim pela transformação direta de base binária para decimal.

   A turma está indicada no 16° byte destacado pela cor vermelha. Temos 01000100 (68 quando convertido para decimal) que corresponde à letra D.

   Por último, o turno, em amarelo, pode ser lido como 01001110 (78 quando convertido para decimal) que corresponde à letra N de noturno.

5. Sim, os dados apresentados são suficientes para preenchimento do campo de verificações. Vamos fazê-lo por partes e em ordem conforme processo descrito na página 49 lembrando que os cálculos são realizados com os valores correspondentes na base 10:

   i) **Verificação da série** - simplesmente escrevemos o número correspondente à série conforme a tabela ASCII. Logo, temos $2 = 00110010$ (50 na base 10) - $v_1 = 50$;

   ii) **Verificação da sigla** - precisamos do produto escalar entre o vetor sigla, $s = (67, 73, 69, 78, 66, 1)$, obtido na terceira questão, e o vetor pesos $p_s = (1, 2, 3, 4, 5, 6)$.

   $$s \cdot p_s = (67, 73, 69, 78, 66, 1) \cdot (1, 2, 3, 4, 5, 6) = 1068$$

   Nosso número de verificação é o resto da divisão desse produto por 131, que é 20. $(20)_{10} = (00010100)_2$ - $v_2 = 20$;

   iii) **Verificação do nome** - o produto escalar entre o vetor nome, obtido na primeira questão, $n = (76, 101, 105, 98, 110, 105, 122, 1)$, e o vetor pesos, $p_n = (1, 3, 1, 3, 1, 3, 1, 3)$ é

   $$n \cdot p_n = (76, 101, 105, 98, 110, 105, 122, 1) \cdot (1, 3, 1, 3, 1, 3, 1, 3) = 1328$$

   Nosso número verificador será v_3 tal que $1328 + v_3$ seja o próximo múltiplo de 131. Então $v_3 = 113$. $(113)_{10} = (01110001)_2$ - $v_3 = 113$;

   iv) **Verificação do número** - a verificação do número é só uma repetição da informação. $(25)_{10} = (00011001)_2$ - $v_4 = 25$;

   v) **Verificação da turma** - mais uma repetição. De acordo com a tabela ASCII, $D = 01000100$ (68 na base 10) - $v_5 = 68$;

   vi) **Verificação do turno** - novamente uma repetição. De acordo com a tabela ASCII, $N = 01001110$ (78 na base 10) - $v_6 = 78$;

   vii) **Verificação da verificação** - aqui nosso vetor verificação é tal que $v = (v_1, v_2, v_3, v_4, v_5, v_6)$ e o vetor pesos $p_v = (1, 2, 3, 4, 5, 6)$, cujo produto escalar entre eles é

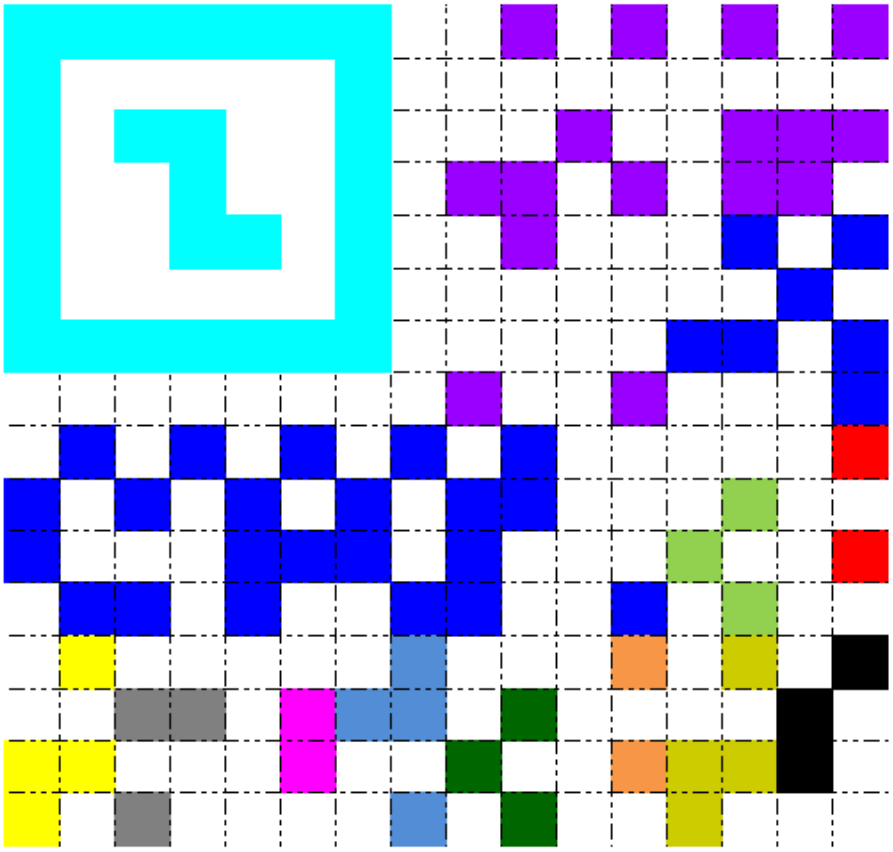
   $$v \cdot p_v = (50, 20, 113, 25, 68, 78) \cdot (1, 2, 3, 4, 5, 6) = 1337$$

   Nosso último número verificador será v_7 tal que $1337 + v_7$ seja o próximo múltiplo de 131. Então $v_7 = 104$. $(104)_{10} = (01101000)_2$.

   Portanto, para João completar o trabalho, basta preencher os bytes vazios com 00110010, 00010100, 01110001, 00011001, 01000100, 01001110 e 01101000 nessa ordem. Uma finalização para o trabalho pode ser dada conforme a figura 6.6.

As tabelas 6.2, 6.3 e 6.4 apresentam o passo a passo para a obtenção dos números verificadores da sigla, nome e da própria verificação.

Figura 6.6 – Homenagem a Leibniz.



Fonte: feito pelo autor.

Tabela 6.2 – Verificação da Sigla.

Vetor sigla	**67**	**73**	**69**	**78**	**66**	**1**
Vetor pesos	1	2	3	4	5	6
Produto	67	146	207	312	330	6
Soma			1068			
v_2 = resto na divisão por 131			20			

Fonte: feito pelo autor.

Tabela 6.3 – Verificação do Nome.

Vetor nome	**76**	**101**	**105**	**98**	**110**	**105**	**122**	**1**
Vetor pesos	1	3	1	3	1	3	1	3
Produto	76	303	105	294	110	315	122	3
Soma				1328				
Soma + v_3 = múltiplo de 131				1328 + 113 = 1441				
v_3				113				

Fonte: feito pelo autor.

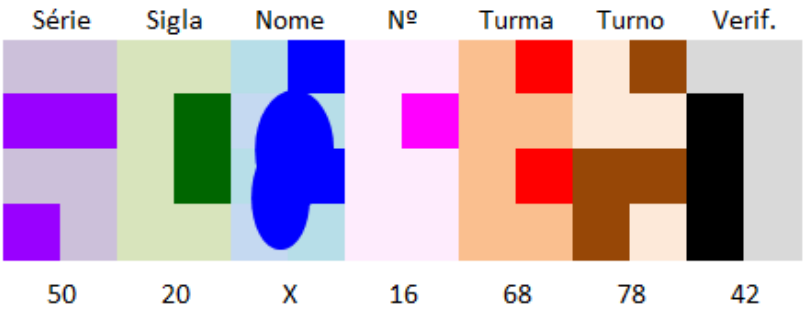
Tabela 6.4 – Verificação da Verificação.

Vetor verificação	**50**	**20**	**113**	**25**	**68**	**78**
Vetor pesos	1	2	3	4	5	6
Produto	50	40	339	100	340	468
Soma	1337					
Soma + v_7 = múltiplo de 131	1337 + 104 = 1441					
v_7	104					

Fonte: feito pelo autor.

Um segundo grupo homenageou outro matemático (figura 6.8). Pedro ficou responsável por colorir a parte de verificações, mas acabou borrando o campo que verifica o nome do "aluno" como mostrado na figura 6.7. Supondo que todos os demais campos estejam corretos, ajude pedro a refazer o byte manchado.

Figura 6.7 – Parte de Verificações.



Fonte: feito pelo autor.

Perguntas:

1. O número que está faltando poderia ser negativo? Poderia ser 150? Justifique.
2. Seria possível descobrir o valor do byte borrado apenas por meio dos outros valores já apresentados no campo de verificação?
3. Qual o número está faltando (borrado) e qual a sua representação binária?

Soluções:

1. Não, o número que está faltando não poderia ser negativo e nem 150, pois é o resto da divisão resultante de um número natural por 131 (algoritmo para verificação do nome) e, portanto, seu valor é maior ou igual que 0 e menor que 131.
2. Sim, é possível. Conhecendo o algoritmo que determina o último número do código (verificação da verificação) e chamando o número desconhecido de x temos a seguinte

equação:

$$50.1 + 20.2 + x.3 + 16.4 + 68.5 + 78.6 + 42 = n.131; \quad x, n \in \mathbb{N}$$

3. Para encontrar o número que está manchado, podemos resolver a equação apresentada na questão anterior.

$$50.1 + 20.2 + x.3 + 16.4 + 68.5 + 78.6 + 42 = n.131$$

$$1004 + 3x = 131n$$
$$x = \frac{131n - 1004}{3}$$

Lembrando que x e n são números naturais e que $x \leq 130$, podemos supor valores para n. Não é difícil perceber que $131n \geq 1004$, logo $n \geq 8$. Seguindo esse raciocínio, encontraremos $n = 10$ e $x = 102$.

Finalmente, $(102)_{10} = (01100110)_2$.

Figura 6.8 – Homenagem a Gauss.

Fonte: feito pelo autor.

6.2 Caça ao Tesouro

A brincadeira de caça ao tesouro é bastante conhecida e pode ser facilmente encontrada na internet. Apesar das variações que podem ser adotadas, a brincadeira consiste basicamente em se chegar a um objetivo principal através da resolução de desafios (charadas ou dicas) que são espalhados e escondidos de forma que cada um leve sucessivamente ao próximo até o desfecho da brincadeira. A atividade é muito simples e toda a diversão está em procurar as pistas e solucionar os enigmas.

6.2.1 Desenvolvimentos

Nessa atividade, o QR code será utilizado para armazenar as dicas ou desafios. Para tanto, é conveniente que os alunos estejam familiarizados com sua leitura e criação, como vistas no capítulo 4, e possuam celulares com câmera ou smartphones capazes de realizar a leitura deles.

Umas das partes mais complicadas no Caça ao Tesouro costuma ser a criação das pistas que levarão ao encontro das próximas e, por fim, ao "tesouro". É aqui que entra nossa confecção e leitura de QR codes. As pistas podem ser inseridas em códigos QR e afixadas na escola e suas imediações, sem deixar de considerar a segurança e o bom funcionamento da instituição durante a brincadeira. Dependendo da disponibilidade de internet, os códigos podem ser de texto ou levar a sites e blogs com resolução online de atividades, questões e explicações mais complexas, imagens ou ferramentas de controle, por exemplo.

Outro fator determinante para essa atividade é que as charadas podem se relacionar a qualquer assunto que o professor esteja trabalhando e tenha vontade de reforçar. Se as respostas para as questões forem numéricas, pode-se estabelecer um "livro código" em que cada número corresponda a uma palavra que junto com as outras formarão uma frase determinante para atingir o objetivo principal. Por exemplo, se a resposta de uma das charadas for 453, e na tabela de códigos (previamente estabelecida) o número 453 estiver relacionado à palavra "*prateleira*", o jogador precisará das outras pistas para completar a frase "*O prêmio encontra-se na terceira prateleira da estante de troféus da biblioteca*".

A localização da próxima pista pode ser dada por um método semelhante como palavras de uma segunda coluna da tabela de códigos ou mesmo passada pelos supervisores condicionadas à resolução da atividade. Outra vantagem desse método, é que mesmo que as últimas pistas sejam encontradas acidentalmente, muito provavelmente será necessário retornar e encontrar uma grande quantidade delas para formar uma frase coerente.

No tópico seguinte, apresentamos o exemplo de um suposto professor que ao terminar o conteúdo de sequências e progressões, queria aliar descontração, tecnologia e revisão de conteúdo em uma atividade diferente. A tabela apresentada mostrará poucas

palavras, mas pode muito bem ser ampliada e adaptada para uma atividade maior e evitar tentativas de localização apenas pela leitura da mesma. Palavras repetidas, números grandes ou que representam mais de uma palavra são recursos válidos.

6.2.2 Exemplificando

Em uma primeira parte o professor pode pedir uma pesquisa sobre os QR codes focando em pontos como: o que são? Como surgiram? Como funcionam?

Nesse momento o professor pode propor questões sobre progressões aritméticas aos estudantes com base nas versões do QR code:

Perguntas:

1. Sabendo que existem 40 versões do QR code em que a primeira tem 21x21 módulos, a segunda 25x25 e assim sucessivamente até a quadragésima versão de 177x177 módulos, que relação podemos estabelecer entre as versões de um QR code?
2. Quantos módulos tem a versão 37 do QR code?
3. Qual é o número da versão composta por 157x157 módulos?
4. Seria possível estabelecer uma relação entre o número da versão e o número de módulos? Se sim, como seria essa relação?

Soluções:

1. Espera-se que o aluno seja capaz de perceber que o tamanho, MxM, da versão cresce em progressão aritmética de razão 4 e assim, chega-se à resposta: as versões do QR code formam uma PA de razão $r = 4$, $(21, 25, 29, ..., 177)$;
2. Temos uma PA em que $a_1 = 21$ e $r = 4$. Usando a fórmula do temor geral de uma PA, temos:
$$a_n = a_1 + (n-1).r$$
$$a_{37} = 21 + (37-1).4$$
$$a_{37} = 165$$
Ou seja, a versão 37 é composta por 165x165 módulos;
3. De maneira análoga temos: $a_1 = 21$, $a_n = 157$ e $r = 4$. Logo
$$a_n = a_1 + (n-1).r$$
$$157 = 21 + (n-1).4$$
$$157 = 21 + 4n - 4$$
$$n = 35$$

4. Considerando-se o tamanho MxM da versão V, podemos chegar facilmente à identidade $M = 4V + 17$ através do desenvolvimento e simplificação do termo geral da PA de primeiro termo 21 e razão 4. Fazendo $M = a_n$ e $V = n$ temos:

$$a_n = a_1 + (n-1).r$$

$$M = a_1 + (V-1).4$$

$$a_n = 21 + 4V - 4$$

$$M = 4V + 17$$

Depois desse rápido "aquecimento", podemos dar início à brincadeira. A divisão em grupos parece apropriada.

Primeiro apresentamos o quadro de conversão dos números em palavras, explicando que cada dica será a resolução de uma questão. Neste exemplo, utilizamos questões encontradas em BEZERRA e PUTNOKI (1994) e PAIVA (1995). Os números encontrados serão convertidos pelo quadro 12 em uma palavra que indicará a localização da próxima dica e assim por diante. A primeira pista (figura 6.9(a)) pode ser entregue pelo próprio professor para familiarização e esclarecimentos iniciais.

Quadro 12 – Códigos do Tesouro.

1	Sob a/o	**11**	Porteiro (a)	**21**	Cantina	**31**	Lixo
2	Sala	**12**	Cozinhero (a)	**22**	da, de, do	**32**	Ventilador
3	Sobre a/o	**13**	Está/é/fica	**23**	Biblioteca	**33**	Cadeira
4	Portão	**14**	Estante	**24**	Livro	**34**	Mesa
5	das/dos	**15**	Prateleira	**25**	Professor	**35**	Professora
6	Alunos	**16**	em, na, no	**26**	Diretor	**36**	Diretora
7	a/e/o	**17**	Banheiro	**27**	Quadra	**37**	Pátio
8	Professores	**18**	Bolsa	**28**	Quadro	**38**	Auditório
9	Diretores	**19**	Mochila	**29**	Computador	**39**	Laboratório
10	Prêmio	**20**	Tesouro	**30**	Troféu	**40**	Matemática

Fonte: feito pelo autor.

Questões:

1. **Pista 1** - Quais são o primeiro e nono termos da sequência $(1, 1, 2, 3, 5, 8, ...)$?

2. **Pista 2** - Qual o próximo número da sequência $(61, 59, 53, 47, 43, 41, 37, 31, 29, ...)$?

3. **Pista 3** - A soma dos 3 primeiros termos de uma PA é 15. Determine esses termos, sabendo que o 3° é o quádruplo do 1°.

4. **Pista 4** - (Vunesp) Um coronel disporá parte de seu regimento num triângulo completo, colocando um homem na primeira linha, dois na segunda, três na terceira e assim por diante. Forma então um triângulo com 231 homens. Qual o número de linhas?

5. **Pista 5** - Quanto tempo um montanhista levará para completar uma trilha de 960 m se percorrer 512 m na primeira hora, 256 m na segunda, 128 m na terceira e assim por diante?

6. **Pista 6** - (Fuvest-SP) Atualmente 50% das gaivotas de certa região são brancas e 50% são cinzentas. Se a população da espécie branca aumentar 40% ao ano e a da espécie cinzenta aumentar 80% ao ano, qual será, aproximadamente, a porcentagem de gaivotas brancas daqui a 2 anos?

7. **Pista 7** - Some todos os números válidos encontrados na caçada até aqui e divida o resultado por 43. O resto dessa operação será o primeiro termo de uma PA de razão 3. Determine os 7 primeiros termos dessa progressão.

Soluções:

1. **Solução - Pista 1** - Trata-se da sequência de Fibonacci, que começa com os números 1 e 1, e cada termo subsequente é sempre a soma dos dois números anteriores. Assim, temos $(1, 1, 2, 3, 5, 8, 13, 21, 34, ...)$ de onde concluímos que o primeiro e nono termos são, respectivamente, 1 e 34.

   Consultando o quadro 12, obtemos a correspondência $1 = Sob\ a/o$ e $34 = Mesa$, que ao ser percebida, espera-se que leve à procura da segunda pista (figura 6.9(b)) afixada **sob a mesa** do professor.

2. **Solução - Pista 2** - Parece uma pergunta fácil, porém, pode-se levar um tempo até perceber que são todos números primos. Na sequência decrescente de primos, o próximo número é 23 e a palavra a que corresponde no quadro é *Biblioteca*. Os que conseguirem chegar à solução do enigma deverão, portanto, procurar a próxima pista (figura 6.9(c)) na **biblioteca**.

3. **Solução - Pista 3** - Podemos escrever a_1, a_2 e a_3 como $(x - r, x, x + r)$, montar um sistema simples e resolvê-lo. Porém, aqui, vamos aproveitar para relembrar uma propriedade interessante que afirma que se a, b e c, nessa ordem, são termos consecutivos de uma PA, então b é a média aritmética entre a e c. Isto é,

$$b = \frac{a + c}{2}.$$

Escrevendo a_3 em função de a_1, $a_3 = 4a_1$, e a_2 como média aritmética de a_1 e a_3 temos

$$a + \frac{a + 4a}{2} + 4a = 15$$

$$a = 2$$

Fazendo as devidas substituições, temos $a_1 = 2$, $a_2 = 5$ e $a_3 = 8$. Convertendo pelo quadro 12 encontramos $2 = Sala$, $5 = das/dos$ e $8 = Professores$, indicando que a próxima pista (figura 6.9(d)) encontra-se na **sala dos professores**.

4. **Solução - Pista 4** - Trata-se de um problema de soma dos termos de uma PA. Considerando as linhas como termos da progressão temos (1,2,3,4...) que representa uma PA de razão $r = 1$ e primeiro termo $a_1 = 1$. Também temos a informação que a soma de todos esses elementos resulta em $S_n = 231$. Basta substituir os valores conhecidos na fórmula da soma:

$$S_n = \frac{(a_1 + a_n).n}{2}$$

$$231 = \frac{(1 + a_n).n}{2}$$

Porém, ainda temos duas incógnitas. Para eliminar esse impasse, escrevemos a_n em função de a_1, da razão e de n. Logo,

$$231 = \frac{(1 + 1 + (n - 1).1).n}{2}$$

$$462 = n^2 + n$$

Que resulta na equação quadrática $n^2 + n - 462 = 0$, cujas raízes são -22 e 21. Como somente 21 se constitui uma resposta aceitável, pelo quadro 12, a próxima pista (figura 6.9(e)) estará na **cantina**.

5. **Solução - Pista 5** - Temos uma PG de razão $q = \frac{1}{2}$, cujos termos são $512, 256, 128, 64, ...$ Se na primeira hora ele percorre 512 m, na segunda 256 m, na terceira 128 m e 64 m na quarta, nesse intervalo de 4 horas ele terá percorrido exatamente 960 m $(512 + 256 + 128 + 64)$.

Outra maneira de solucionar a questão é substituir os valores conhecidos na fórmula da soma dos termos da PG:

$$S_n = \frac{a_1.(1 - q^n)}{1 - q}$$

$$960 = \frac{512.\left(1 - \left(\frac{1}{2}\right)^n\right)}{1 - \frac{1}{2}}$$

$$480 = 512.\left(1 - \left(\frac{1}{2}\right)^n\right)$$

$$\frac{480}{512} = 1 - \left(\frac{1}{2}\right)^n$$
$$\frac{15}{16} - 1 = -\left(\frac{1}{2}\right)^n$$
$$\left(\frac{1}{2}\right)^n = \frac{1}{16}$$

De onde concluímos que $n = 4$ e portanto o tempo para completar o percurso será de 4 horas. Consultando o quadro 12, o próximo destino é o **portão**. Lá, encontrar-se-á a sexta pista conforme a figura 6.9(f).

6. **Solução - Pista 6** - Embora essa questão possa ser solucionada inteiramente de maneira algébrica, uma forma bastante eficaz de resolvê-la é atribuindo valores. Se 50% das gaivotas são brancas e as outras 50% também, podemos dizer que 100 gaivotas são brancas e outras 100 cinzentas. Se uma grandeza cresce 40%, podemos dizer que ela foi multiplicada por um fator de 1,4. Logo essa será a razão da PG que representa as gaivotas brancas, que pode ser expressa por $(100, 140, 196)$. Analogamente, para as gaivotas cinzentas teremos o fator de multiplicação 1,8 e a PG $(100, 180, 324)$.

   Ou seja, passados dois anos, as gaivotas brancas serão em número de 196 e as cinzentas de 324 totalizando 520 gaivotas. Assim, o percentual de gaivotas brancas será dado por $\frac{196}{520} = 0,3769...$ que corresponde, aproximadamente, a 38%.

   Não deve ser difícil perceber que 38 é o número que usaremos para consulta no quadro 12. Fazendo a correspondência ($38 = \textit{Auditório}$), podemos ir em busca da sétima e última pista, figura 6.9(g).

7. **Solução - Pista 7** - Os números encontrados nas soluções das pistas 1, 2, 3, 4, 5 e 6 são respectivamente 1 e 34; 23; 2, 5 e 8; 21; 4 e 38. Somando-os todos obtemos 136, cujo resto na divisão por 43 é 7. Assim, nossa PA de razão 3 será $(7, 10, 13, 16, 19, 22, 25)$ que analisada à luz do quadro 12 revelará a mensagem **"o prêmio está na mochila do professor"**.

As imagens a seguir, são as pistas em códigos QR para fixação nos lugares escolhidos.

Figura 6.9 – Pistas do Caça ao Tesouro.

(a) Pista 1

(b) Pista 2

(c) Pista 3

(d) Pista 4

(e) Pista 5

(f) Pista 6

(g) Pista 7

Fonte: Códigos gerados pelo site http://mqr.kr.

7 CONSIDERAÇÕES FINAIS

Como vimos, o interesse pelos códigos é muito antigo e possui uma história bastante rica. Aproveitando-se do interesse que pode ser despertado por tais assuntos, o professor pode usá-los tanto no auxílio de alguns conteúdos específicos quanto para demonstrar a importância e aplicabilidade da matemática nos diversos campos.

Couto (2008) afirma que desde pequenos somos acostumados a montar cifras bastante básicas e que hoje é praticamente impossível vivermos sem um bom código, principalmente no tocante à privacidade. Ressalta ainda que essa preocupação vem desde a antiguidade com a invenção de muitas cifras e códigos utilizados e esquecidos ao longo do tempo. Situação que, segundo Brasil (2000, p. 13), dentro de uma contextualização sócio-cultural, ajuda a "compreender as ciências como construções humanas, entendo [sic] como elas se desenvolveram por acumulação, continuidade ou ruptura de paradigmas, relacionando o desenvolvimento científico com a transformação da sociedade."

A história está repleta de exemplos que podem servir de partida para uma atividade em classe ou demonstração da importância da matemática e sua relação com outras ciências e assim, em sintonia com o apontado em Brasil (2000), conhecer e utilizar a ciência como elemento de interpretação e intervenção, reconhecendo seu sentido histórico, bem como da tecnologia, e percebendo seu papel na vida humana em diferentes épocas e a capacidade de transformação do meio pelo homem.

Nos exemplos vistos, é marcante a presença de cifras e de criptografia que se constituem como ferramentas de ensino igualmente poderosas. Porém, apesar da confusão e mistura que frequentemente ocorre entre códigos, cifras e criptografia, há, como foi visto, diferenças entre eles. Neste trabalho, enfatizamos a presença diária dos códigos, principalmente do código de barras e sua notável evolução para o QR code.

Infelizmente, muitas vezes, a matemática por trás dessas "ferramentas" foge do conteúdo e ensino propostos e é preciso que o professor saiba dosar seu estudo para não gerar um resultado oposto ao desejado. Um resultado que ao invés de motivar o aluno por meio da curiosidade, acabe por desinteressá-lo com mais complicações.

Contudo, para além das propriedades aritméticas e outras que podem ser abordadas na utilização de códigos como ferramenta de estudos, chamamos a atenção para ideias simples que fazem grande diferença, como a possibilidade de identificar o início e o fim do código apenas observando a quantidade de algarismos ímpares ou pares. Mais impressionante ainda é a ampliação do código pela inserção de um dígito oculto resultante dessa mesma paridade. Já no QR code, notamos essa engenhosidade na leitura que é feita e significado atribuído para um conjunto de bits dependendo da posição em que se

encontram.

Nada impede que conhecimentos ou conteúdos mais complexos sejam explorados, mas, em ambos os casos, podemos facilmente abarcar competências e habilidades preconizadas pelos Parâmetros Curriculares Nacionais como a leitura e interpretação de textos em representações matemáticas como tabelas, gráficos, equações, fórmulas e muitas outras, além da possibilidade de estimular o trabalho em equipe e cooperação por meio das atividades propostas.

> Quando, por exemplo, são propostas atividades coletivas, de cooperação entre estudantes e de elaboração de projetos conjuntos, quer se tornar o aprendizado das Ciências e da Matemática mais eficaz, mas, ao mesmo tempo, quer se promover o aprendizado do trabalho coletivo e cooperativo, como competência humana. Aliás, são absolutamente raros os trabalhos demandados na vida real que não exijam precisamente atividades conjuntas e cooperativas. (BRASIL, 2000, p. 54).

Portanto, vemos que não é preciso esperar por um tema específico ou um trabalho que traga questões dos conteúdos mais comuns do ensino fundamental e médio. O professor pode introduzir as relações entre a matemática e o dia-a-dia em um projeto, em uma brincadeira ou espaço de distração como no caso da caça ao tesouro. Ainda que muitas vezes de forma imperceptível, acreditamos que essas relações reforcem conteúdos básicos, estimule o raciocínio e principalmente, propiciam um ambiente acolhedor e divertido para os alunos que frequentemente não esperam nada mais que assuntos difíceis, cálculos laboriosos e risco de reprovação nas disciplinas de exatas.

REFERÊNCIAS

BEZERRA, M. J.; PUTNOKI, J. C. *Novo Bezerra Matemática*: 2º grau - volume único. São Paulo: Scipione, 1994. 213-229 p.

BRASIL. Ministério da Educação. Secretaria de Educação Média e Tecnologia. *Parâmetros Curriculares Nacionais (Ensino Médio)*, Brasília: MEC, 2000.

CALSSEMAN, B. American Mathematical Society - AMS. *How to Read QR Symbols Without Your Mobile Telephone*. Disponível em: <http://www.ams.org/samplings/feature-column/fc-2013-02>. Acesso em: 8 de julho de 2016.

COUTO, S. P. *Códigos e Cifras - da Antiguidade à Era Moderna*. Rio de Janeiro, RJ: Novaterra, 2008.

EBY, C. *QR Code Tutorial*. 2015. Disponível em: <http://www.thonky.com/qr-code-tutorial/>. Acesso em: 8 jul. 2016.

ECKSCHMIDT, T.; MORITA, S. S. *QR Code - Comunicação e Engajamento na Era Digital*. Estados Unidos: Moderattus, 2014. E-book. ISBN 978-1502559791.

EVES, H. W. *Introdução à história da matemática*. 5ª. ed. Campinas, SP: Unicamp, 2011.

FINI, M. I. Revista do Professor - Atualidades. *Controle dos Códigos de Identificação*, SEESP, n. 2, p. 70–80, 2009.

LAVOR, C. C. et al. *Uma Introdução à Teoria de Códigos*. São Carlos, SP: SBMAC, 2006. Notas em Matemática Aplicada; v. 21.

LIPSCHUTZ, S.; LIPSON, M. L. *Álgebra Linear*. 4. ed. Porto Alegre, RS: Bookman, 2011.

MELLO, J. L. P. Aritmética modular e sistemas de identificação. *Revista do Professor de Matemática - RPM*, Sociedade Brasileira de Matemática, São Paulo, SP, n. 48, p. 22–26, 2002.

MILIES, C. P. A matemática dos códigos de barras. *Revista do Professor de Matemática - RPM*, Sociedade Brasileira de Matemática, São Paulo, SP, n. 65, p. 46–53, 2008.

MILIES, C. P. Breve Introdução à Teoria dos Códigos Corretores de Erros. In: *Colóquio de Matemática da Região Centro-Oeste*. Campo Grande, MS: UFMS, 2009. Disponível em: <http://www.sbm.org.br/docs/coloquios/CO-1-09.pdf>. Acesso em: 9 jul. 2016.

MILIES, C. P. A matemática dos códigos de barras: detectando erros. *Revista do Professor de Matemática - RPM*, Sociedade Brasileira de Matemática, São Paulo, SP, n. 68, p. 28–42, 2009.

PAIVA, M. R. *Matemática*. São Paulo, SP: Moderna, 1995. v. 2. 9-60 p.

QR code. In: WIKIPEDIA: the free encyclopedia. Wikimedia, 2016. Disponível em: <https://en.wikipedia.org/wiki/QR_code>. Acesso em: 8 jul. 2016.

SANSWEET, J. *Introducing the QR Code*: The reality and the magic. Aukland: ProofreadNZ, 2011. E-book. ISBN 978-0-473-18451-3.

SHANNON, C. E. A mathematical theory of communication. *Bell System Technical Journal*, 1948.

SOS. In: WIKIPEDIA: the free encyclopedia. Wikimedia, 2016. Disponível em: <https://en.wikipedia.org/wiki/SOS>. Acesso em: 8 jul. 2016.

TOLEDO, F. *Sáquele jugo a los Códigos QR*: Conozca el potencial de escanear códigos qr en los smartphones. [S.l.: s.n.], 2012. E-book. ASIN B008BID85M.

VENTURA, J. Notas de Combinatória e Teoria dos Códigos. In: Departamente de Matemática. Instituto Superior Técnico. Lisboa, 2013. Disponível em: <https://www.math.tecnico.ulisboa.pt/~jventura/CTC/CTCnotas.pdf>. Acesso em: 9 jul. 2016.